DDoS Attack Mitigation

Description: Steve and Leo discuss Apple's response to the FBI's court order, the hack of the Linux Mint distribution, more Comodo bad news, a major cryptoware ransom paid, and follow-ups on the glibc and Apple Error 53 stories. Then Steve details everything that has transpired since last week's "GRC Is Down" episode.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-548.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-548-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is back. So is GRC.com. He's going to talk about DDoS mitigation. Also, Steve's take on the Department of Justice versus Apple. You'll be interested to hear what he has to say about it and a whole lot more. All the security news coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 548, recorded Tuesday, February 23rd, 2016: DDoS Attack Mitigation.

It's time for Security Now!, the show where we talk about your security online. Boy, there has never been a more important time to be talking about security than right now. And fortunately we - you know what's great is we've been doing this long enough now - Steve Gibson is here - for 10 years, 11 almost. We've been doing it long enough now that we've set kind of a basis of understanding for the conversations that we have now.

Steve Gibson: Right.

Leo: So if you haven't listened since Episode 1, before you listen to this episode - no. But it's a good idea, go back, because all of these are still timely and topical, and we cover a lot of fundamental technology like encryption.

Steve: Right. Well, for example, we'll be talking about some details of the way iOS9 works, or iOS sort of generically, which is covered in detail, I think it was either a two- or three-podcast series we did on iOS security, when Apple finally published a very comprehensive whitepaper with the release of iOS7 [SN-446, SN-447, SN-448]. And so we walked through all of that, which is why I remembered some things that are relevant

to today's discussion about Apple versus the FBI and the whole question about what is it that the FBI wants, how much of this is Pandora's Box being opened and so forth.

And our position is, or my position, at least, is I'm no one to speak on policy, but there are specifics of the way the technology works. And one of the things that just - I cringe when I hear people loosely using ill-defined terms like "backdoor." That's the favorite term. But there's no good definition for backdoor. And I would argue that, in this particular case, what we're talking about is some changes to sort of soften the front door that already exists, that - well, anyway, I'm getting ahead of myself. But we've got a great podcast. GRC is back on the air.

Leo: Oh, yes, I noticed that.

Steve: And so today's podcast is titled DDoS Attack Mitigation. I want to talk, I want to sort of recap the last week, since last week's podcast, which was "GRC Is Down," and explain why I've done nothing. That is, it's not some magic that I've pulled off. It's nothing that I've done. But there are serious reasons why I have chosen to do nothing because choosing to do something would dramatically impact some aspects of GRC that I'm reluctant to do, I mean, eliminating services and giving others control of my certificates. And when I hear from the industry, "Oh, everybody does it," it's like, well, I don't care. I'm not doing it.

So anyway, I think a really interesting back half of the podcast to explain what was going on, how Level 3 has just been amazing through this, and they really stepped up and helped a lot. But I think our listeners are going to find it very interesting to sort of go inside DDoS attacks today and what it means to deal with them because it severely cramps what we would be able to do. So that's great.

And we've got a bunch of news of the week, including the Apple versus the FBI, the hack of the Linux Mint distro, more bad news from Comodo, the very expensive ransom paid by the Hollywood Presbyterian Medical Center. Dan Kaminsky of DNS spoofing fame has weighed in on the glibc flaw since it is DNS related. And of course some follow-up on the Error 53.

So I think a great podcast for people. And I really think people are going to find the DDoS Attack Mitigation conversation interesting. And, boy, did I learn a lot about the industry and this podcast in the last week, which I will tell everyone about.

Leo: Ah. Can't wait to hear it.

Steve: It was phenomenal the way the industry and our listeners stepped up. People were buying redundant copies of SpinRite to support me through this.

Leo: Oh, isn't that nice?

Steve: I mean, I'm humbled by it. It was just phenomenal. And turns out all of Level 3 engineering and security listen to the podcast. So I didn't need to explain who I was. They were like, wow, you're on the phone?

Leo: We've heard of you.

Steve: And everybody in the industry who's in the mitigation business offered me their services for free.

Leo: Of course they did. Of course they did.

Steve: And they said, Steve, we'll waive our fees. We'd like you to, you know, if you need our help, you've got it. I just - I was overwhelmed by the response. And so anyway, we'll talk about more of that in the second half.

Leo: As they should, and as you should...

Steve: I was just humbled.

Leo: Yeah. It's a nice feeling, isn't it, when you call for support - I've had this happen a few times - and they go, "You use our product? Oh, what can I do?" That's always a nice feeling.

Steve: So our Picture of the Week.

Leo: Oh, I love this, yeah.

Steve: I tweeted this. It's been around the 'Net. It's of interest if someone's been living under a rock for the last week or isn't a member of Twitter or somehow hasn't seen this, a great cartoon titled "Pandora's iPhone" that shows a picture of Tim Cook in the lead, reaching for the backdoor's knob. Behind him stands the FBI. Behind him even bigger is hackers. Behind them is a crazy guy dressed up as a general, labeled "Repressive Regimes," and then a group of others labeled "Etc." So the point being, are we opening Pandora's iPhone by having Tim Cook unlock the backdoor?

So what the court order has asked Apple to do is to modify iOS, create a modified iOS or a shim or something, essentially altering the way the current software works. As we all know, you have, typically, a 10-mistake lockout on guessing the unlock code for the iPhone. And if you can't get it within that allotted number of guesses, what will happen is the phone will then proactively wipe out the symmetric encryption key which drives the cipher between storage and the CPU. I remember hearing Jeff last week sort of puzzled about, wait a minute, it decrypts your phone every time you unlock it and then re- it's like, well, no.

As we know, listeners to the podcast probably understand how current whole-drive encryption works. And that is that the drive is always encrypted, and it is decrypted on the fly, under the influence of a symmetric key, as data is read from it, and then reencrypted as data is read back. So with the simple act of destroying, just zeroing one small bit of memory, the contents can never be recovered. And as far as we know, that

symmetric key is generated by the phone and at no point ever leaves the phone. There's no reason not to believe that's the case. So the idea is we absolutely have to prevent that from happening.

So the court has ordered Apple to assist the FBI by disabling the 10 wrong guesses lockout, which is presumably enforced by software, not hardware, thus subject to being changed. There's also, in addition to an 80-millisecond, hardware-enforced, delay in trying a guess, there is additional software-induced, per-attempt delays to slow down guessing. So they want that removed, also. Again, it's software induced, so that could be removed.

And then, finally, they want an electronic avenue for submitting their guesses, that is, we're talking about brute-forcing this passcode. So rather than having some poor intern sitting there, you know, 000000, 000001, 000 and so on, they want to be able to just hook it up to a brute-forced generator and have it run at the maximum speed it can, which is 80 milliseconds per guess, without any downside, without the 10-mistake lockout and with no additional delay. So of course Apple is saying, no, we're going to do everything we can to fight that.

So I don't take any position in this. I mean, the reason that this has all been, I mean, we have been talking for the last few months that this is going to be the year where this begins to happen. And everyone who's been following the podcast for long will remember that I suspended my work on CryptoLink because I could read the handwriting on the walls. It's like, I didn't want to invest all of my time to create a super great commercial product to have it be outlawed because there's no way I'm going to produce a VPN that has a backdoor or a weak front door or any kind of a door. So this has been in the air for a while.

What we do know, though, is - and there is a lot of misinformation on the technical side. And as I said at the top of the podcast, one of the problems is people who don't understand the technology are loosely using ill-defined terms. I mean, "backdoor" is sort of a catchall, which means whatever the person saying it wants to mean. So we have a problem with inexact terminology being used by non-technical people such as politics and technology and the collision thereof.

Here's what we know about the way the iPhone and iOS devices work today. And I verified in the September 2015, so only a few months back, iOS9 security whitepaper that it hadn't changed, and it's the same as what we discussed back with iOS7. And that is - and I remember at the time remarking how surprised I was, but pleased, about Apple's super tight architecture. And listeners will remember that I came away feeling very bullish about the incredible focus that Apple had clearly put into securing the iPhone and iOS devices for its users. The iPhone or iOS device, in this case an iPhone, will periodically, even when locked - and that's a misconception that I've seen on the Internet. It's like, well, no, it won't update unless it's unlocked. No, it will update locked. If the phone is locked and on WiFi, it will periodically check for updates.

The iPhone sends its unique device ID and a randomly generated nonce, a number used once, to Apple. Apple, if it wants to send the iPhone something it will accept, must take the device's unique ID and the nonce, bundle that with the update package, and sign it with Apple's super secret private key, and send it back to the phone. The phone verifies that the signature is correct because it's got Apple's matching public key burned into its boot ROM. So it verifies that the signature is correct, and then verifies that the nonce that it has received in this package is the same one that it just sent, and that the unique device ID matches.

So back when we discussed this several years ago, I remember saying, wow, that means that every single update is customized. And Apple did this for a reason, and we talked about it then. We would want to prevent an older version of iOS that was for some other device, not this particular one, from being essentially cross-installed, thus allowing a downgrade attack to recreate flaws that were now well known in the earlier versions, but had been fixed in later versions. So Apple took on the burden of not being able to mass distribute any of their iOS updates. Every single one is generated, custom, in answer to a request from the device, signed with Apple's private key, in order for the device to accept it.

So this puts to rest that the question technically - not politically, not policy-wise, but technically - can Apple, if they choose to, respond uniquely to this singular request and provide the FBI, either in their facility or remotely, with a piece of software that answers the court's demand, that is absolutely not reusable ever again, not even ever again on the same device because the nonce protects reuse. So one time, answering this phone's request, generating software that can only be used that time on that device. And that's the way the system is now.

So I understand that there are huge broader questions that I completely get, like the whole slippery slope argument, that if Apple does it for this, then we already know, for example, that the DA back on the East Coast has said he has 175 other phones waiting to be opened. So Apple used to do this, and we talked about it, how there was a multi-month backlog in phones that Apple was working through to crack the code and unlock the phone. Apple decided they didn't want that business.

So I just wanted to put to rest the technology is sound. They beautifully designed this. And what it does give them is, if they choose to, the ability to open this single phone in a way that, even if they gave the software to the FBI - and one report I read said that the FBI was going to give Apple the phone so that Apple could do this to it, and then the FBI would take it away and do this brute-forcing for however long it took. So it's not even the case that Apple would, like, lose control of that update. They're being asked to essentially weaken the front door, which is normally locked tightly enough that no one can get in without the phone destroying its contents by wiping that symmetric key.

And where we go from there, nobody knows. It's a fascinating issue of our time, and we're in no position to dictate policy. But that's the way the technology works. It does not create - there's all kinds of analogies now floating around. Being asked to cut the ribbon that protects the phone, or being asked to give the FBI a ribbon-cutter that allows them to cut the ribbons on all other phones, that's not at issue. Apple must sign with their private key a per-instance and per-device software update for the device to accept it.

Leo: And we should point out that it doesn't require precedent for all these other district attorneys with locked attorneys to go and request the same thing of Apple. They all can do the same.

Steve: Right.

Leo: I mean, they're watching with interest. It would make it easier if they had a federal precedent. But there's no reason for them not to seek a decision, as well.

Steve: Oh, I completely agree. I mean, this is a big issue. And NPR did a piece interviewing Senator Angus King, who is an independent, very rational on this. And his point is that this should not be an issue where the court forces Apple's conduct. This properly should be Congress looking at this and then deciding to set the law so that from this point forward this is the law of the land. And I agree. I think that, I mean, this is really important. We don't want some random judge to say, oh, yeah, my nephew is with the FBI, and so I'm going to sign the order and good luck.

Leo: Right. Do you want me to play the clip from Senator King?

Steve: I don't think...

Leo: All right.

Steve: Yeah, I don't think we need to. For anyone who's interested, the link is in the show notes. And I did create a bit.ly link. It's very good. It's 4.5 minutes long. I do commend it to our listeners. It's bit.ly/sn-548-2, again, sn-548-2. And it's -2 because there's also a -1, which is sort of the dark side. That's a similar NPR interview of Manhattan's District Attorney Cyrus Vance, Jr., who of course explains that he's got - he has some numbers. He has something called a "cyber lab." And of the 500-some phones they have, 175 they can't get into. And he very much wants precedence to get set here so that they can send a big carton of phones to Apple to have them all opened up.

Leo: I support Apple, well, we'll see what Apple's - we, by the way, don't know what Apple's response is. I'm glad Tim Cook wrote the open letter at Apple.com because that has raised this wonderful conversation. We don't know if Apple's going to say no. Apple may well say, yeah, fine. They have a couple of days to respond left. I think the 26th they have to respond.

Steve: Yeah, they got a three-day extension.

Leo: Yeah. I don't, you know, I think what - in my opinion, Apple should pursue this so as to nail it down, to get the court decision and, in fact, if they have to go to the Supreme Court, get the court decision. But I do feel like one of the reasons that this is a good case is there's not a huge amount of urgency. The two shooters are dead. We should point out the law does not protect the privacy of dead people. Furthermore, that phone is owned by the government, by San Bernardino County.

So really this is a nice test case because a lot of the confusing issues are out of it. It's merely that, should Apple, if they have the ability, should they unlock this phone, and would that be an undue burden for the FBI to ask them to do that. That's what the judge is going to rule on is, is this too burdensome. And so we should get that. But I feel like Apple should do it. I mean, given what you've just said, that this is just a one-time-only deal, why shouldn't Apple do it? Once they get the decision.

Steve: Yeah, I mean, they clearly don't want to. And then, of course...

Leo: They don't want, I understand, they don't want to get in the business of doing this.

Steve: Well, right. Although somebody, I think it was during This Week in Google last week, I think it may have been Jeff, someone I think brought up the very good point that, if Apple sells iPhones to China, and Apple is selling iPhones into China, and wants to, that the phones being sold there must abide by Chinese law. And there's no doubt, I think, that the Chinese government would want the same sort of access into the phones of Chinese citizens that our own law enforcement is asking for, in apparent bulk, into the phones of U.S. citizens. So exactly as you said, Leo...

Leo: Again, a negative outcome. But should we decide on how we prosecute criminals based on what another nation might do? I mean, yes, it's a negative outcome, but Apple's chosen to do business in China. That means they have to adhere to the law of China, period. It's not an option. Same with Google and everybody else. In fact, that's one reason Google pulled out.

Steve: One way to look at this is that Apple wasn't quite clever enough with the security. I'm impressed that the FBI figured out what to ask for, that sort of softening of the front door.

Leo: But we should point out that you can encrypt and all that stuff. But if it's a four-digit passcode to unlock it, it's a weak password.

Steve: Right.

Leo: It's nice that they have the delay in there. It's nice that they have the 10-try wipe, although that's not on by default. You have to turn that on. Four-digit passcode is weak. That's why Apple made it six. Is six weak? Yes.

Steve: Yup. Yup.

Leo: It's not as good as a password.

Steve: In fact, I have obviously been a little preoccupied in the last week, but I was thinking it would be fun to enhance the Password Haystacks page with an 80-millisecond per guess field, so that it would show you...

Leo: How long it takes, yeah.

Steve: ...how long your iOS password would take the FBI to crack it at maximum cracking speed.

Leo: If Apple turns off all the other...

Steve: If, yeah, exactly.

Leo: The five-second delay and all that.

Steve: If Apple were to make it possible. I mean, I imagine that, in retrospect, Apple is now sorry that they can do this.

Leo: Right. This is what I brought up on MacBreak Weekly. I bet you they're working real hard right now to make it so that they can't be asked to do this again. And I am sure future versions of the iOS will prevent this whole issue from coming up because they'll - they can...

Steve: Unless Congress decides that...

Leo: They have to put a backdoor in.

Steve: ...the contents of phones are like the contents of homes, where a search warrant permits access to the contents.

Leo: Right.

Steve: And as I have mentioned on previous...

Leo: And that's, by the way, that's the conversation we need to have.

Steve: Yes.

Leo: All of this is really secondary to the larger conversation, which is how the phone should be protected.

Steve: Right.

Leo: And this is something, you know, same thing with email. Your mail at work is protected. Your physical mail is protected. Your boss can't open your letters. But the boss can open your email. So the boss can't listen in on phone calls. If it's personal, they're supposed to hang up. But they can read everything you do on the computer. So the law has not caught up with the digital world. And the rules for the digital

world are currently different than they are for the physical world. And that's really what needs to be happening here in the long run is Congress needs to step forward and say, okay, here's what the rules are for digital. And are they the same?

Steve: And let's also remember that the software industry as a whole is living in some amazing bubble because the license agreements that we click on say we're not responsible if the wheels fall off, you are. And, by the way, this is not really yours, we're just giving you a license to it. But at the same time, good luck. If the wheels fall off of a car, then the manufacturer is responsible. Not the software industry. We've been in this bizarre land where it's just - and I don't know how it's persisted as long as it has. But it's like, eh, if it works, great. If it gets infected with malware, well, we're sorry about that, hope you can recover your losses.

Leo: Good luck.

Steve: Okay. Amazing.

Leo: Yeah. Really, it's a fascinating subject. And I think now that we've had a week to think about it, I think we've kind of boiled it down a little bit better than the initial reaction to it. And I hope people are listening and paying attention.

Steve: Well, you and I are powerless to affect the outcome. All I wanted to clarify was that, from a technology standpoint, Apple could do this one. But I fully understand that, if they can do one, then Cyrus has got 175 more. He's just rubbing his hands together, can't wait to send them off to Cupertino.

Leo: But I should point out he doesn't have to wait. He can ask right now. I don't know why he hasn't.

Steve: There is another piece. Apple has about a dozen orders which have not generated this much press. They've already, from last year, there's about 12 other court orders that Apple has been fighting that are pending.

Leo: Right.

Steve: But because it wasn't San Bernardino and Farook and the business phone, and it wasn't a hot button, it was just some random who knows what that didn't really rise to the level. This is the case - some people are arguing, in fact, from a political standpoint, that the FBI chose this. Remember that this phone hadn't been backed up in six weeks. This was Farook's business phone. His personal phone was physically destroyed and is absolutely uncrackable. I mean, it's gone. The contents are destroyed.

I'm distracted because GRC is now under denial of service attack, so...

Leo: Oh, of course, they waited till the show, yeah. It probably will be a little one.

Steve: Well, we'll talk about that. But anyway, so...

Leo: No, there's little copycat attacks. We had one that was a little copycat attack. It was very easy to remediate.

Steve: So, yeah, I am distracted.

Leo: Sorry. You want to take a break?

Steve: It's all right.

Leo: You can take a break. I can do an ad or something.

Steve: There's a big red band that is now moving across the screen. So what was I saying? Farook...

Leo: Well, I think that - go ahead.

Steve: So there's been an argument that the FBI chose this for its powerful political impact, in order to use it as a wedge issue for Apple; whereas the other 10 or 12 pending court orders that they have just didn't generate any attention.

Leo: And I really, really, really like the kind of the bottom line that over now five shows we've come up with, which is that what has to happen is the courts and probably Congress need to decide how do you treat a smartphone. Given that our lives are on there, our health information, our pictures, everything we care about we are now storing on a notably insecure device that's fully connected to the Internet at all times, can be lost, has a camera, a microphone on it, and a GPS, how do you treat this? Is this special? Is this different than a safe in my basement? Because we know what the law is about a safe in my basement. How is this protected? Should this have higher protection than a locked safe in my basement? Because currently it does, technologically.

Steve: Right. And the problem is the technology provides absolute protection.

Leo: Right, right.

Steve: And that we know, that math is perfect. We can create uncrackable cryptography. So the question is, I mean, so this creates a new problem that we have never had before

because, when the authorities have a search warrant for someone's home, if they don't willfully open the front door, well, we've all seen "CSI," you know, they take a battering ram and blast the door open in order to enter. So the crypto creates the opportunity for perfect protection. We're going to have to have a law that determines, is the fact that we can create perfect encryption, does that mean that Apple and other U.S. manufacturers can offer perfect encryption in the United States without there being the provision for law enforcement to have access?

Leo: Good.

Steve: Okay. So for anybody who downloaded last Saturday, February 20th, a copy of the Mint distribution of Linux, hopefully you already know that the ISOs were replaced with a backdoored version of the operating system. A hacker who goes by the name of Peace was interviewed over an encrypted chat by Zack Whittaker of ZDNet. Zack writes ZDNet's Zero Day column. This hacker by the name of Peace told Zack that a few hundred Linux Mint installs were now under their control. So there were more than a thousand downloads that day.

And what happened was the ISO was modified so that a backdoor known as Tsunami was present in that system. And so if you updated or installed the Mint distro from this compromised version, the Tsunami malware would connect to a specified IRC server and await commands. So it could be used for DDoSing, for downloading other programs into that system for subsequent execution, and can even remove itself to remove traces that it had been there.

And what I got a kick out of was that the hacker also said that they "used their access to the site to change the legitimate checksum - used to verify the integrity of a file - on the download page with the new checksum of the backdoored version." Which I remember when GRC decided to grab the TrueCrypt archive, and I got the Defuse.ca site to host the hashes for the downloads because it never made any sense to me that, on a page where you were downloading something, that page would say here is the MD5 or the SHA-1 hash for the download because, if the site was compromised, well, any hacker worth their salt would change the supposedly correct hashes to match the malware. Which these guys did.

So it certainly makes sense for the hashes to be located in some different location, some different website, so they can't both be compromised at the same time. Anyway, the site was brought down. The problems were found. The distribution has been cleaned up. There was something about them still having potential control of the admin control panel for the site in case they wanted to, like, get up to more mischief in the future.

Leo: After this happened - I use Linux Mint, and after this happened...

Steve: Yeah, and I've heard you talk about it.

Leo: And then somebody else posted an article which was listed on Hacker News saying here's why I don't use Linux Mint for any reason, and was a fairly compelling argument that Clem, the lead guy, is really not paying too much attention to security in general. And so I've abandoned Linux Mint, which is a shame because it is easily

the most Windows-like of Linux versions, very straightforward, comes with a lot of not-free software, which makes it easy for people. And I've rolled back, not even to Ubuntu, but all the way back to the original Debian distribution, which is not as easy to install, not as beautiful for people, although it can be made to be. But it's far more secure, and I'm much happier with it, frankly.

Steve: And in fact the last audit says that there are about six million instances of Linux Mint out in the world.

Leo: Yes, it's very popular. It's the number one, you know, because it's based on Ubuntu, which by itself is very nice and easy to use. But they've added things like - you'll love this. They've added Flash and Adobe PDF Reader. They've added stuff to make it easier, codecs and things. But...

Steve: Yeah.

Leo: They also - the real issue is a more technical issue which has to do with upstreaming and how they've made it hard to update a lot of software. And that's a security problem because, if that software should have a security flaw, most cases with a good Linux you can update it. These, some of the updates, or many of the updates are blocked because they've modified software. And so the fact that you're not getting downstream updates is not a good idea.

So all in all I was convinced. And there's lots of good distributions. In fact, there's some very good secure Linux distributions, a new one that just came out which sandboxes all the apps. It's in beta right now. I just read about it, and I'm very intrigued. I've downloaded the beta ISO, and it's quite solid and nice. You know, someday we'll get you on Linux.

Steve: Probably.

Leo: Or you like FreeBSD, too.

Steve: I do.

Leo: Which is built to be secure.

Steve: Yup. So Comodo is back in the doghouse. Tavis Ormandy, our...

Leo: Again?

Steve: Yes, again, with another bloodcurdling problem. Tavis continues to look at it, and he posted again in the Google Security Research blog where he does his work. He said

when you install Comodo Internet Security - which, you know, that's their package that they're pushing, and that's the thing that installs the Chromodo browser that we talked about before which completely shuts down all, basically, browser security guarantees.

So now, Tavis writes, when you install Comodo Internet Security in the default configuration, an application called "GeekBuddy" is also installed and added to - and this won't make sense to non-Windows people, but HKLM\System\CurrentControlSet\Services, meaning that GeekBuddy is installed as a background hidden service. I mean, all services are kind of hidden. They just run. They start up when you boot, and they're always there running behind the scenes. But GeekBuddy is a tech support application that, as Tavis writes, "uses a number of questionable and shady tactics to encourage users to pay for online tech support."

And then in the Bug Report he gives a link to the GeekBuddy page from Comodo. And I went over it because I was curious; and it's like, oh, you've got to be kidding me. First of all, $200 a year they're charging for GeekBuddy access. So even without subscribing, this thing installs in your system and runs as a service. But I didn't get to the best part. He says: "As has been noted by numerous people over the last few years, GeekBuddy also installs a VNC server and enables it by default." So VNC, of course, is a popular free remote desktop facility to allow remote access to your machine. So installing this gets you ready for GeekBuddy and sets it up, even if you have no intention, don't even know it's there, and have no intention of paying Comodo $200 a year for GeekBuddy support.

Leo: What? My god. The thing is, you can check a box that says don't install GeekBuddy, but I don't think you can check a box that says don't install VNC.

Steve: So, again, just - the only takeaway is that everybody within reach of this podcast should stay as far away from Comodo as they possibly can because, I mean, I don't know where they're getting their stuff. But they are not behaving in a responsible fashion. And of course it is the most security you can have and, like, blah blah blah. It's like, okay, yeah, except that nothing that they're doing supports that claim.

In the news was a $17,000 ransomware payment made after 10 days of being locked out of all their patient data by the Hollywood Presbyterian Medical Center. In a published statement, Allen Stefanek, the president and CEO, wrote: "The first signs of trouble at HPMC came on February 5, when hospital employees reported being unable to get onto the hospital's network. Our IT department began an immediate investigation and determined we had been subject to a malware attack. The malware locked access to certain computer systems and prevented us from sharing communications electronically. Law enforcement was immediately notified. Computer experts immediately began assisting us in determining the outside source of the issue and bringing our systems back online."

Leo: The first thing the computer experts said is, "So, where do you keep the backups?"

Steve: Yeah, exactly. And I love this: "The hospital staff was forced to move back to paper and transmit information to doctors and others by fax machine" - yes, we got out our stone knives - "while the IT team and outside consultants struggled to restore the network."

Leo: I hope that IT team has been fired.

Steve: Oh. "Eventually, hospital executives decided" - basically after 10 days, and the IT people said all your files are encrypted; we can't help you. So eventually, he writes, "hospital executives decided that the quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this."

Leo: Unbelievable.

Steve: So it made the headlines.

Leo: Unbelievable.

Steve: And this is certainly not the last such high-profile attack of this sort that we're going to see. It's just, unfortunately, it used to be that it was fun to infect machines. Viruses propagated just to show that they could. Then, over time, they've gotten increasingly aggressive. But, boy, when you have bitcoin - oh, and this was - it was paid in bitcoin. I have it in my notes here. Oh, 40 bitcoin was the ransom. So 40 bitcoins at today's going rate is $17,000 U.S.

Leo: Unbelievable. They should have waited another week, it would have been cheaper.

Steve: Yeah, I think maybe that the hospital, with waiting 10 days [crosstalk], probably said...

Leo: Maybe that's why they were.

Steve: Oh, wow.

Leo: Keep waiting, it'll go down some more.

Steve: So Dan Kaminsky has weighed in on the glibc flaw. There's a beautiful graphic that, frankly, it's so big that it couldn't fit without pushing the text out of a good pagination. So I thought, okay, we can survive without it. But basically it's a dependency tree showing glibc's - showing all of the GNU ecosystem's dependents. And essentially glibc is in the center, shining like a bright sun, with all of these tendrils reaching out. Basically everything in the ecosystem, with very few exceptions, has a direct connection. Glibc, the GNU C library, is in everything, as we said last week.

So of course Dan is the person we talked about years ago who discovered the problem with low entropy in DNS server port choice, and there's a 16-bit ID that queries are

generated with. And he found that there was poor entropy there, and also poor entropy in the ports that they were using. And what that allowed was spoofing of DNS replies. And of course that gave birth to GRC's DNS Spoofability Test, which allows anyone to use the facility on our site to test the spoofability of whatever DNS servers they're currently configured to have resolving their DNS, which is exactly what you want.

Anyway, I'll just share the first two paragraphs of what Dan wrote. His posting was titled "A Skeleton Key of Unknown Strength." And he said: "The glibc DNS bug is unusually bad. Even Shellshock and Heartbleed tended to affect things we knew were on the network and knew we had to defend. This affects a universally used library (glibc) at a universally used protocol (DNS). Generic tools that we didn't even know had a network surface are thus exposed, as is software written in programming languages designed explicitly to be safe. Who can exploit this vulnerability? We know unambiguously that an attacker directly on our networks can take over many systems running Linux. What we are unsure of is whether an attacker anywhere on the Internet is similarly empowered, given only the trivial capacity to cause our systems to look up addresses inside their malicious domains."

Second paragraph says: "We've investigated the DNS lookup path, which requires the glibc exploit to survive traversing one of the millions of DNS caches dotted across the Internet. We have found that it is neither trivial to squeeze the glibc flaw through common name servers, nor is it trivial to prove such a feat is impossible. The vast majority of potentially affected systems require this attack path to function, and we just don't know yet if it can. Our belief is that we're likely to end up with attacks that work sometimes, and we're probably going to end up hardening DNS caches against them with intent rather than accident. We're likely not going to apply network-level DNS length limits because that breaks things in catastrophic and hard-to-predict ways."

So what he's essentially saying is that, as we discussed last week, if a device generates a DNS query, somebody malicious on that network that sees the query can respond to it probably before the true DNS server gets the query, looks it up, and responds. So somebody on the same network, or present in the traffic, has this, as Dan confirmed, almost absolutely exploitable opportunity. But the way, as we know, the system works, the Internet works, most devices are configured to use some remote DNS resolver. They ask that DNS server, which Dan refers to as a "cache," which it technically is, to go look up the IP on their behalf.

So the point is that a remote attacker that was answering queries with a malicious packet would probably be defeated by it having to go through that intermediary DNS server. That is, the DNS server would get it and cache it, and it's probably going to be a malformed reply, which would crash the Linux machine that asked, if it could get to the Linux machine. But unfortunately it gets to the intermediate DNS resolver and goes no further because the DNS resolver looks at it and goes, what the heck is this, and just throws it away.

So again, we talked about it last week. This was deep and pervasive, and it was going take a while for the industry to sort through what exactly this means. We know that we want to immediately fix this so that all of the different things that use glibc are recompiled with updated patched versions that don't have this problem that's been around for eight years, since 2008. But in the meantime we're looking for real-time mitigation.

The good news is most instances, it looks like, the attacks that have been designed are stopped by an intermediate cache. Most real-world environments do have an intermediate cache. But at the same time, as Dan wrote, it's one thing to stop the

attacks we know. It's another thing to - and we haven't yet been able to, we the industry, prove that it isn't possible to sneak an attack through a cache by having it look like a valid reply, but which also still performs an exploit when it is forwarded then to the original requesting system.

So just, wow, interesting and scary that this kind of flaw can exist and be just incredibly pervasive. And again, this is why all of these Internet-connected devices have to be able to have a means of updating themselves. It looks like this is not compromising everything that's on the Internet, thanks to the intermediate DNS cache architecture. But it's still certainly a local network attack. And until things get patched, we're vulnerable in any sort of a local network situation.

I heard you talk about Error 53. For those of our listeners who haven't heard the news, Apple said, whoops, we're sorry. I have just a very short quote from the support note that Apple put up. They said: "After you try to update or restore your iOS device in iTunes on your Mac or PC, you might see Error 53 in iTunes and 'Connect to iTunes' on your device. Error 53 appears when a device fails a security test. This test was designed to check whether Touch ID works properly before the device leaves the factory, and wasn't intended to affect customers.

"For anyone who experienced Error 53, Apple has released an update to iOS 9.2.1 to allow you to successfully restore your device using iTunes on your Mac or PC. Use the steps in this article to restore and recover your device. If you believe that you paid for an out-of-warranty device replacement based on an Error 53 issue, contact Apple Support to ask about reimbursement."

So they really stepped up. And it looks like we got a little carried away, the industry, in being as upset as we were; and Apple quickly said, oh, yikes, we never intended this to inconvenience customers.

Leo: As Rene Ritchie said, it actually was intended to be a factory error only that would show a failure of, I don't know, the pairing of the Secure Enclave, I guess.

Steve: Right.

Leo: And the idea was, oh, we'll see it at the factory and not ship that phone.

Steve: Yeah. Yeah. It seems to be that the system knows if you change or remove the Touch ID. And the YouTube video that I referred to last week, the woman that was doing this with her stereomicroscope and doing surgery on the flex circuitry in the iPhones said that she'd even relocated the chips onto a different piece of flex circuitry in order to try to move the Touch ID functionality, and somehow it knew, so she hadn't fooled it, whether it was done right or not.

But the idea was you either changed the Touch ID, or you just removed it. You spilled something on it, it got into the little crack of the button, the button stopped working, and then you said, hey, you know, I want my phone fixed. And so they said, well, we can't fix the Touch ID. We'll give you a new home button, but the Touch ID won't work. And people would say, yeah, okay, fine. And then the problem was, as we know, the next time they updated iOS, iOS freaked out because suddenly there was no Touch ID button, when that was supposed to be a factory event which got out into the marketplace.

Time for miscellaneous. I have three little goodies. This is completely random, but my very favorite certificate-issuing company in the world, everybody knows, is DigiCert. They're the people that make our certificates. I just happened to see a tweet go by this morning that they're looking for a new customer relations intern. So I just thought, hey, I'll give them a little wider audience. I created a bit.ly link, bit.ly/digicertjob, D-I-G-I-C-E-R-T-J-O-B. And they're located in Utah, with lots of benefits and skiing and a nice environment. So if anyone is interested is a customer relations intern job at DigiCert, I just thought, well, what the heck. I'll give them a little bump.

And David Needle died.

Leo: Yeah.

Steve: I just sort of wanted to note his passing. He was a friend. He was at IDG. He'd been in the personal computing business way in the early days. I thought I remembered him writing up about my light pen for the Apple II. And so I just googled "David Needle LPS II Light Pen," and it came right up, his very flattering write-up of the development work that I did in the design of the light pen. And he must have been my age. So I hate it when I see anyone young...

Leo: He was a little older than you, but he was still pretty young. I think he was 70. But he was pretty young, yeah.

Steve: Oh, okay, yeah. A veteran of the industry.

Leo: Mm-hmm.

Steve: And third random miscellany is, oh my god, TiVo just got instant commercial skip. Have you seen that, Leo?

Leo: Mm-hmm. I've used it.

Steve: Oh. I cannot believe how well it works.

Leo: Not me, no, I haven't used it.

Steve: Really?

Leo: I would never skip commercials.

Steve: It's funny because they offered another piece of hardware, like maybe six months ago, that had that feature, like you had to buy that version. It's a weird wedgie sort of

TiVo thing that offered commercial skip. They called it Skippy or something, I don't know [Bolt]. And I kind of was looking at it, thinking, well, why can't I have that on my TiVo? Well, it appeared.

Leo: I don't know how they get away with it. I mean...

Steve: I don't either.

Leo: We'll see what happens. You can disable it. I think that's how they get away with it. Notice not everything is skip-enabled.

Steve: True, true. It's funny, too, because I didn't understand what it was, but I was seeing these little green skip tags. And I thought, what the heck is that?

Leo: This is such a good job. You press whatever it is, the "D" button, and it just goes to the beginning of the next segment of the show.

Steve: It's amazing.

Leo: What?

Steve: It's amazing.

Leo: You know what? I bought another TiVo. Lisa said, "I want that." So we're replacing the Xfinity X1 box in the gym with a TiVo Roamio Pro.

Steve: Yeah.

Leo: TiVos are so good.

Steve: I'm back to TiVo. They've just nailed it. They have the third-party apps. You can do Hulu and Netflix and everything else. And, I mean, even when you had to zip through at high speed through the commercials, it was like, okay, this is better than having to watch them. But now, oh, goodness.

Leo: That was the main reason is that on the Xfinity X1, you start the fast-forward, but then you can't stop it, so it keeps going all the way to the end of the show. Or you do rewind, and it keeps - it was so funky flaky bad that we just - it was so frustrating. So she said, "Well, can't we have a TiVo in here?" I said, "Honey, those are expensive." She said, "Buy one." They're worth it. They're worth it.

Steve: And lastly...

Leo: Yeah.

Steve: Just a quick - was this a tweet? No, this was email I wanted to share. It had just a couple different things in it. Frederick Pollock, who's in Goodrich, Michigan, he said, "No, I'm not on Flint water." So, good, Fred. You don't have lead poisoning, hopefully. And the subject line said "Zeo still available on eBay 02/10/2016 as of 9:00 p.m. Eastern time."

Anyway, he wrote, "I just watched your latest podcast on TWiT. I thought I had missed my chance to get a Zeo. Not true. $40, and it's on its way. Great podcast, Steve and Leo. I've been a listener from almost the first one. I use a Roku now. The app works great. Thanks again."

And finally he says, "I have owned SpinRite for years and cannot count the number of creaky hard drives it's brought back to life," he says, "(just like the Terminator movie). They just get up and go again. Sometimes it gets a little scary, like a zombie you can't kill. Good zombie, good zombie, LOL." So, Fred, thank you for the nice note.

Leo: All right. We're going to talk about DDoS attacks. You want to check your server? Is it still redlined?

Steve: I turned the screen off, actually, because I...

Leo: Didn't want to see?

Steve: I didn't want to look at it.

Leo: We'll talk about all of the pros and cons of remediating broken websites. But first...

Steve: Yup, attack is still underway.

Leo: Yeah.

Steve: So our attacker has just demonstrated that he's listening to this live.

Leo: I guess so.

Steve: Well, no. Because the moment you asked me whether we were still being attacked, I said yes. And at that moment the attack stopped.

Leo: Really. Can they do it that fast, on a dime like that?

Steve: Yes.

Leo: If he's got a botnet, I guess he issues a command; right?

Steve: So I am talking to the attacker and to the Security Now! audience both.

Leo: Interesting. Hello, attacker.

Steve: So first off...

Leo: Don't you have homework to do?

Steve: First off, many people, I will just say again, so that I make sure we don't run out of time. I was overwhelmed by the industry's response, both the Internet industry, the listeners to the podcast, I mean, who indicated they would walk through fire in order to keep GRC viable and on the 'Net. I was just, I mean, I was humbled by it way more than I expected. And so thank you. I'm proud that we've built this relationship that we have, really.

And, wow. Level 3 has just been amazing. I'm on a first-name basis with all kinds of people. Bryce, Brandon, Sharon, Lee, Tim, Robert, and others, you all know who you are because I've talked to you many times in the last week. And I will explain why I had so many conversations with Level 3. But again, as I just demonstrated, or as our attacker just demonstrated for us because we were off the 'Net again, I did nothing to attempt to mitigate this DDoS attack, or series of attacks. And I'm going to explain why, because to do so requires some significant changes in GRC's network. And so I want to - I think everyone is going to find this interesting and probably learn something, sort of from my viewpoint, from someone who's running a site, who has the particular profile that GRC does, which is different than other websites.

So just to recap briefly, the first time I saw this attack was Saturday before last, around 3:30, I think it was, in the afternoon. I was actually visiting my sick neighbor where he was convalescing. And when I came home, we were off the 'Net. That attack lasted, I think it was about 90 minutes. Then there was a gap, and then a 60-minute attack, and then about three more hours that brought us into the evening of Saturday, and we went off the 'Net again with another attack. At that point I wasn't sure what was going on. I had gone to the datacenter, and I remember reporting to our listeners that what I saw was a DNS reflection.

Now, I don't know if the - it looked like later attacks had larger bandwidth. So it may have been only a DNS reflection attack. What Level 3 later told me, when they took a look at the traffic, was that it was the kitchen sink. There was all kinds of other things that were in place, flooding us. So I talked last week about having asked Level 3 to filter out incoming DNS to port 53 of the GRC.com IP that was under attack. Now, the problem was that we were sharing a router with a bunch of other Level 3 customers.

Leo: Oh, that's too bad.

Steve: Yes. And that router had a 10Gb link to the rest of Level 3's network, and the attacks were larger than 10Gb. In fact, I remember looking at the traffic at the end of last week's podcast and seeing in the chart that Level 3 had, I think it was 12.875 or something gigabits, billion bits per second, of traffic. Well, that couldn't come down the 10Gb link. So what was happening was the attack on us was affecting the neighborhood. It was adversely affecting the connectivity of the people that we were sharing that router with.

Leo: Could you tell it was aimed at you and not somebody else on that router?

Steve: Well, yes. That's a very good point. When I looked at the traffic, it was aimed at 4.79.142.200.

Leo: Your IP.

Steve: That's the IP for GRC.com.

Leo: Got it.

Steve: Okay. So as we've talked about in the past, denial of service attacks are, you know, in the old days - there's been a huge evolution in them over time. In the old days there was the original sort of TCP SYN flood, where TCP SYN packets, SYN short for synchronize, would be sent to a server, and it would assume that a TCP connection was going to be set up. So it would allocate memory to handle that connection and respond with a SYN-ACK.

The problem was, if the source IP was spoofed, it would send the SYN-ACK off to a spoofed source IP. But it would leave that memory allocated and assume that the packet got lost. So it would wait a while, then retransmit the SYN-ACK to respond to the incoming SYN, then wait a longer while and try again, and wait a longer while and try again. Meanwhile, more SYNs are coming in, representing, it thinks, more pending connections. So it keeps allocating memory for each one of these and finally crashes the server, the server itself, which is no longer able to accept any more incoming connections.

So that's old school. And in fact I independently solved the problem, and Dan Bernstein had also solved it, with something called SYN cookies. And so I proposed a solution and was told, hey, you know, Gibson, that already exists. It's like, oh, okay, well, I didn't know that. So great minds.

So what's happened since is that we've gone from a situation like that, where one attacker could generate so many pending connections that a server would come down. Servers have since been hardened against a TCP SYN flood like that, where it's really not many, you don't need many SYN packets per second in order to bring down a server's ability to make new connections. Now we've gone just to massive, just overwhelming

bandwidth. Thus the 12- to 13-billion bit per second flood that this attacker has been hitting us with intermittently since Saturday before last.

So one problem is that, as was the case where GRC is sharing, it's a so-called "Edge router" - Verio called it an "aggregation router" - with other customers, it could affect people who were not being attacked. The other problem is that, when you're buying bandwidth, as GRC is, from a Tier 1 provider, we're buying it on something known as the 95th percentile basis. It's also called 95/5. And we've talked about this in the past, Leo, when we've talked about attacks, where victims of long, protracted attacks find themselves hit with a massive bandwidth bill because you're charged for the attack bandwidth.

And so anyway, the consequence is that it's necessary to stem this attack. And so this is done with a process known as "null routing." If you picture, for a second, Level 3, a big, global, Tier 1 Internet backbone provider. We've talked often about peering relationships, where Level 3 will peer with AT&T and with Sprint and with all the other major Tier 1 providers, so that customers in each other's network are able to reach resources in the other ones. And so those are peering relationships. The peering relationship is physically a Level 3 router and some other Tier 1 provider's router sitting in the same rack.

Or, for example, I think One Wilshire is a major interchange in Los Angeles, where everybody's got a presence, and they agree that they're going to interconnect their routers. So they run fiber optic cable between the Level 3 router and the Sprint router, and the Level 3 router and the AT&T router, and that's the peering relationship. So presumably a DDoS attacker, distributed denial of service, has a widely scattered bot network under their control and is able to command those remotely controlled bots to send traffic to a target IP, as has been the case, GRC.com. So that traffic enters Level 3's network all over the place, through all of those peering points connecting it to other networks, and maybe from some customers inside Level 3.

All of those Level 3 routers have, as we've discussed, routing tables that, when a packet comes in, the router's job is to figure out where to forward it to. It'll have multiple interfaces to other routers. And so it looks at the destination IP and sends it toward its destination.

So what happens during an attack that is protracted is I get on the phone, and I've got a whole bunch of phone numbers now, and dial this, then this, then this, and get to here. And then I say, "Hi, it's me again." And they go, "Hi, Steve." They always say, "How you doing?" And I say, "Well, you know, it occurs to me that I've had 10 years of problem-free service. I should have called from time to time just to be able to say how happy I am with the flawless connectivity and the great service that Level 3 has provided over the last decade. But as it happens, I only call when I have problems. So at the moment I'm not doing so well."

And they say, "Okay, what do you want to do?" And I say, "GRC.com is under attack. Let's null route it." So what that means is that they type some things into some magic admin system that they've got, and this propagates to all of the routers on their border, and presumably some intermediate routers. And the way a routing table works is that, when you have a series of routes defined, aimed at different interfaces, the job of the router is to match the most specific route. Meaning that, for example, GRC.com's IP is 4.79.142.200. So 4.79 dot anything dot anything, that's a bunch of IPs, presumably all sort of located in the same region of Level 3. So any incoming packet bound to 4.79 dot anything is sent down in that direction. But if there's a more specific route, if there, for example, is an exact route 4.79.142.200, that supersedes the less exact match.

And so what Level 3 does is they route that to nowhere, to the null zone. Basically, it tells every router, everywhere on the perimeter, drop incoming packets. And so the beauty of that is they never have a chance to aggregate down to a high-bandwidth flow. At all the peering points, the routers get their tables updated with this so-called "null route," which exactly matches the IP, and thus the traffic goes no further. It just dies.

So the good news is the traffic has been terminated. The bad news is I have no idea whether the attack has been terminated because there's no visibility into the attack at that point. So I've acted as a good citizen and told Level 3, stop sending bandwidth to me. But the flipside is I now have no idea how long that null route needs to stay in place. So in one instance GRC.com was null routed. Or GRC.com was under attack. Because that flooded the router, all of our network was down; and, as we know, some of the neighbors were adversely affected.

And what happened Saturday night was that the IP Group in Level 3, which is a different group than the group that I normally talk to to handle the DDoS and security stuff, they saw that there was an inordinate amount of traffic, and they just shut down the interface. So they proactively took us offline because, I mean, the traffic wasn't doing us any good anyway, and they had to preserve the integrity of the connection for the people we shared the router with. Which I have no problem with. I was going to be offline anyway.

So the next morning I started to fire up relationships with Level 3, and that's how I was pleased to learn that they knew me because they listen to the podcast, and they're listening to this now. And they probably know that we just had an attack.

Leo: Hi, Level 3.

Steve: And that the attacker is listening to the podcast, as well. So I had them instead - we brought the interface back up, but null routed GRC.com. Now, the reason we did that was that the website is actually on www.grc.com, which is at .202. So all of the routers dropped the traffic to .200. But since I had long ago moved the web over to www, we popped up on the Internet. And things were good, but not for long, because this attacker was watching what we were doing and switched the attack over to www.grc.com, and we were down again. So I called Level 3 again, went through the Centrex dialing, get to the person you want to talk to.

And I think this was Brandon that I was talking with several times at this point. And he said, "Oh, you're back." I said, "Yeah, we're down again." I said, "My guess is" - and I had never gone back to look at the traffic again. I said, "The website's back down. It's probably www.grc.com, .202. Let's null route that." So that was null routed. But now, again, that's our web traffic, so we're off the 'Net again, but the newsgroups were up. And I've talked often about GRC's newsgroups, which is yet again on its own IP, news.grc.com. And so I was able to have some dialogue in the newsgroups until that went down.

So it's like, I called Brandon again. I said, "Okay, I give up. Let's just null route the entire network because we're off the 'Net, and I want to be responsible." And so the point was that you can not only null route individual IPs; but, for example, a /29 network is a block of eight, and so that's the block that I've got. So that encompassed starting at GRC.com on through the rest.

So the details of the last, like of last week are a bit of a blur. But the good news was that

the attack wasn't persistent. And, I mean, even when I first talked about this on Tuesday, I'm not sure how much attacking we had had. But it sort of felt like, I mean, I didn't know if the person had an axe to grind or was testing out a new tool, wanted to see, like test GRC's defenses. I mean, again, I had no idea. And in fact, if we had been under pervasive attack, if I was doing this podcast, and we had been completely blown off the Internet on an ongoing basis, I thought, okay, I'm going to create an email alias, steveyousuck@grc.com, to say to the attacker, look, what is this about? What have I done? Why is this going on? Because again, all I want to be is allowed to be on the Internet.

Now, where I want to go here over the next 35 minutes before we run out of time is, like, what it takes to solve this problem in a situation where the attacks are ongoing and persistent, and why I've done nothing, and why I hope that this attacker will leave us alone. I should mention that there have been two brief 10- or 15-minute probes. Saturday night, very, very late, actually early, early Sunday morning, after several days - the last attack that I worked with with Level 3 was Thursday evening. And it was sort of late in the evening. The attack began. I thought, oh, god, okay. So I called Brandon or Bryce or somebody, and I said, okay, take us off. And so we null routed all eight IPs. I had to get some sleep. Shut down, essentially, our network overnight.

Got up in the morning on Friday, made coffee, sat down, called Level 3. I said, okay, and this time I talked to Lee, who was there in the morning, and I said, "Let's see if we can get back on." And so Lee removed the null route, and the attack had stopped. And again, I don't know when. I don't know how long it was because when we're null routed, there's no - I can't tell if we're under attack. So but we were up then all of Friday, all of Saturday.

And then there was a 15-minute, no, this one was a 10-minute probe early, early Sunday morning. At 12:35 to 12:45 we were down. And again, this didn't feel like somebody mad at GRC. It felt like someone wondering whether we were still attackable, whether we could be pushed off the 'Net. And I'm sure they turned their bots on and then tried to get to GRC, and there was no getting to GRC, and so this person turned the bots off. And so that was a probe. And we got another one this morning. From about 1:45 to 2:00 a.m. this morning, a similar short test to see whether we had any DDoS defenses in place.

Leo: So in effect we just told him on the air, oh, hey, we're back. Go ahead, attack us.

Steve: Well, okay. So there's been, I mean, I've been working to sort of divine the intention of this person and what this is about. It's clear that, I mean, I've told the person nothing that they don't already know. They're very competent. They know how to do this. When I null routed an IP or a domain name, the GRC.com, although I lost email because email is at GRC, and DNS, at least the web was up, until he noticed, he or she, whomever, noticed that we were up on www and so that one got attacked. And then when that one got protected, then something else got attacked. And so at that point I gave up.

So there's nothing I'm saying that this person doesn't already know. They understand how this stuff works. Oh, and in fact in the show notes, Leo, if you're interested, I have a snap that I made of this morning's 1:45 to 2:00 a.m. attack, just showing here there's 24 hours of bandwidth, and the 2:00 a.m. outage shown on the graph.

Leo: The red bar you were talking about.

Steve: Right, that's the red bar. And I got a much bigger one that I'm looking at right now.

Leo: Because the scale of this graph is 9Mb? Is that the top?

Steve: Yeah, it dynamically scales. And so that is 9Mb. And as I mentioned last week, I have a 10Mb, what's called a CDR, a committed data rate.

Leo: So it will never exceed 10; right?

Steve: Which is the bandwidth that I buy from Level 3.

Leo: Yeah, right. Wow.

Steve: Okay. So what Level 3 has since done is they have what they call "grooming." They've groomed my bandwidth, meaning that the IP folks said, you know, Steve's having problems.

Leo: He shouldn't have to keep calling us.

Steve: Well, actually, if I'm off the 'Net, I'm off the 'Net. But they didn't, I mean, their bandwidth is amazingly high quality. I mean, in all the years I've just never had any problem. And so they don't want their other customers to have a problem. So essentially they gave me my own port, as they called it, so that attacks on GRC, while they will still be just as disabling to GRC...

Leo: Oh, that makes sense.

Steve: ...they at least won't affect any other customers. And so again, I salute them for this.

Leo: So you're saying all a bad guy needs is the IP address of a website, and he could just launch it against that website.

Steve: Okay. So, yes, in GRC's case. So what has happened is that...

Leo: You want to take - let's take a break.

Steve: Okay.

Leo: You want to take a break?

Steve: Yes, because I have to explain to people why it is not practical [crosstalk]...

Leo: Right, why aren't you doing something about this.

Steve: Yes, why I desperately hope I don't have to do anything because, if I do, ShieldsUP! and DNS Spoofability and all the goodies that GRC offers, and the newsgroups, which are so valuable, not only to me but to a large community, they all have to go away.

Leo: Right. A number of people did say, hey, why doesn't Steve just use SquareSpace?

Steve: Okay. So I heard from a lot of the companies that offer DDoS mitigation solutions.

Leo: Like Cloudflare and those people.

Steve: I did hear from Cloudflare. John said that they'd be happy to...

Leo: John Graham-Cumming, we know him well.

Steve: Yup, exactly.

Leo: Great guy, yup.

Steve: Said that he'd be happy to work with us. I heard from an engineer at Incapsula that offers a similar service. I even got contacted by Russia's largest DDoS mitigator.

Leo: Oh, I bet they're good, actually. They're really good.

Steve: So here's the problem. So what all these services are is known as a reverse web proxy. They put themselves in front of, it would be in our case, in front of GRC's server, and they field all of the traffic. What that means is that we would point our DNS to them, meaning that the IP for GRC.com and www.grc.com would be in the IP space of whatever provider we chose. And then here's the deal breaker for me. They control our domain, and they have the certificate for GRC. That's the way all of these places work. And I said, "Well, uh, sorry, but that's not happening." And the response I got from one of them

was, "Well, everybody else does it."

And it's like, well, okay, okay. I'm not representing to the people who visit my website that they have a secure connection between my server, which I stand by, and their browser. What this means is this is exactly what we're talking about all the time with a corporate appliance in the middle, or in this case an organization in the middle. Suddenly everybody at this third-party DDoS provider has essentially access to the secure traffic to GRC because they interpose themselves, and they terminate the HTTP connection. So they've got a private key for GRC, at least a domain validation certificate, at the minimum, and they can get one because they're able to prove that they have ownership of GRC's DNS because part of the deal is I've given them ownership of GRC's DNS. So again, it is the last thing I hope I have to do.

Now, the only real thing we've got happening is credit cards for eCommerce. And again, yes, everybody does this, but I really hope I don't have to because I would rather be responsible for GRC's security. It's just me. There's no one else, no evil or compromised employee or anything. It's just me.

So the other thing, though, for example, is Perfect Passwords, which is GRC's crazy random number generator that a surprising number of people depend on. I've got tweets from people saying, hey, how can I - "I can't get passwords from Perfect Passwords." Well, I'm uncomfortable with the idea that the passwords they get are being decrypted by someone in the middle, which is part of this bargain, if I were to put GRC's servers behind a reverse web proxy, which is the only way to keep GRC on the 'Net, to keep GRC's web presence on the 'Net in an attack. And, yes, I can do it. Many, many, many companies do. I hope I don't have to.

But there's more because, as I mentioned before the break, ShieldsUP!. The way ShieldsUP! works is a visitor says I would like you to check my ports. I've just set up a new router. I'm over at a client's facility. I want to check their security. I mean, ShieldsUP! has been around for, who knows, I don't know, a decade. And many people depend upon it. But the moment you say "Check my ports," probes come out from our network, from .206. And there's no way to hide them. There's no way to obscure them because I need to send TCP SYNs out in order to see if I get SYN-ACKs back. I drop them, if I do, in what's called a TCP half-open, so I'm not actually opening connections to anyone's ports. I'm just noticing that their port is willing to be opened, and I drop it.

But ShieldsUP! cannot be protected because, exactly as I was saying, this is all about bandwidth. And if there is any physically present IP that an attacker could discover, they simply flood that IP with overwhelming bandwidth. And I have no choice but to shut down, to null route that incoming flood. And I don't know how long it lasts. So I just pull the covers over my head and wait for a while and then bother Level 3 again and say, okay, let's see if it's safe to come back. And it is or it isn't.

Same thing is true for the DNS Spoofability Test. The way that works is I wrote a pseudo DNS server such that, when someone brings up the spoofability page, there's some crazy DNS queries which their DNS server resolves by using a custom, crazy DNS server that I wrote from scratch for this purpose, which fields these queries and looks at the source port and the DNS, I forgot what it's called, the 16-digit ID of the query in order to check its randomness. And we were briefly off the 'Net but looks like maybe we're back. There's somebody else has been attacking us, not apparently the original guy. So unfortunately...

Leo: Sometimes you get copycats, as well, yeah.

Steve: This podcast is causing havoc for us. But I want to explain...

Leo: Any little script kiddie who can figure it out.

Steve: I want to explain to the industry. So none of those services can exist if GRC is going to be attacked. They're free. I'm not making any money from them. I would like them to exist. But I can't be in a situation where I have to run around and monitor the bandwidth constantly in order to null route incoming overflow traffic. In order to be a responsible customer of Level 3, I will have to simply discontinue all of those services. We would neuter ourselves to just being a website.

I looked into what to do with email. Google offers a corporate email service where we could keep our GRC email addresses, but Google would handle it, so they would handle attacks. The point is any publicly exposed server is subject to attack, that is not behind a reverse proxy. And nobody that I could find proxies email. Nobody proxies generic TCP. So again, the newsgroups that are so valuable to me for R&D and development, and to the community that we've created, if there's a server that's on an IP, it can receive incoming attack traffic, and I'd simply have to remove it.

So I have been, essentially, I've been hoping that we would be able to weather these attacks, that whoever it was behind them wasn't determined to force GRC off the 'Net. The only thing that will happen is we will be forced to become a generic neutered website, offering no services, and hiding behind a reverse proxy in order to stay on the 'Net. I'll do it if I have to, but I hope I don't.

So that's the story of the last week. Level 3 has been exemplary. In all the years I've been with them, more than eight, I've never had any interaction with anyone, but they've just been great. At least I know that we're not affecting any other customers right now. I don't know what the future holds. And I did create an email alias, steveyousuck@grc.com. So...

Leo: If the bad guy wants to...

Steve: Yeah, go to a coffee house. I'm sure he can probably create, you know...

Leo: Oh, I think he knows how to do it. He'll use one of those...

Steve: Yeah, an untrackable alias. And I don't care who this person is. Everyone will remember, who's been around for a long time, back in 2001, the first denial of service attacks that we suffered, back when I was with Verio. And it was some bots that were generating non-spoofed traffic. I collected a bunch of packets. I did reverse lookups on the IPs. I found that there were a bunch that were the IP .oc.oc - like oc.oc.cox.net or something. So that said, oh, this is Orange County.

I used my connections with the FBI and had them contact one of the households that was

only four miles away from me who had a bot that was attacking us. And I went there and got a copy of the bot, brought it home, set it up on its machine, essentially creating a honeypot, and let it connect to its IRC server. I then created my own IRC sort of client system in order to get into the IRC chatroom.

I ended up tracking down the kid, whose handle was Wicked. His name was Michael. We talked on the phone a couple times. And I said, you know, "Why are you attacking me?" And he said, "Oh, I heard you were a bad guy." And I said, "I'm not a bad guy. Leave me alone." And I know where he lived. I know who he was. I didn't pursue it because I didn't care. I just, you know, I figured just - I figured communicating with him, I could just say, look, I'm not evil.

Leo: Right.

Steve: So anyway, that's where we stand. I did nothing to mitigate the previous attacks. I hope I am not driven to do so. At some point, if this continues, I'll have to say, okay, GRC is going to lose all the things that it has been able to offer for free because I just won't have a choice. We will have to disappear and hide behind a reverse web proxy and make the best of it. I hope it doesn't happen. We've gone a long time without. But that's the story.

Leo: You could put SpinRite up for sale somewhere else. People say that, if you need the money for SpinRite, you could just put it on...

Steve: No. The point is, I mean, yes, I mean, I can sell SpinRite. That's not a problem. But I can't have ShieldsUP!...

Leo: I understand all the other stuff. Right, yeah.

Steve: Right, right, right. Oh, I'm...

Leo: I'm saying, if it became an issue economically, you could easily sell SpinRite at other places, I presume.

Steve: Well, I guess I don't understand how that's a solution.

Leo: No, it's not. I'm just saying it keeps your income stream going, though.

Steve: Well, frankly, due to the amazing response from our listeners, we ended up doing about the same last week, despite the interruptions, as we did the week before because literally people were buying redundant copies of SpinRite, which, you know, please don't do that. Wait till I have something else to sell and then buy that. I really, I mean, I'm humbled. I'm just stunned by the level of support that was shown.

Leo: People love you.

Steve: I learned a lot about our community.

Leo: People adore you, Steve.

Steve: I was. So I hope that...

Leo: It's what happens because you give so much. You've been doing that for 11 years, you've been giving so much. Of course people want to give back. That's what happens.

Steve: Well, I'm really flattered. I want to thank Level 3. I hope you're listening because everybody there has just been fabulous. I'm so happy. I renewed my contracts with them for another four years a couple months ago because I want to stay there forever. I mean, it's been really, really, really good. And I hope this will pass, and that I can just get back to finishing SQRL and get on to working on SpinRite 6.1. That's what the world wants me to do, and this is a big distraction, which I hope is over. If not, then I'll have no choice but to change who GRC is.

Leo: [Crosstalk], Steve, you're just taking a break. You're having a vacation. You're enjoying life. You have [crosstalk] sipping some wine, going to the beach.

Steve: I have to tell you, Leo, I think our...

Leo: Life's good.

Steve: I think our podcast listeners could hear last week how thrown I was.

Leo: Yes.

Steve: And I said to Jenny, I said, "I don't know, early retirement kind of has a certain appeal to it." You know?

Leo: Uh-huh. I say that, too. I say the same thing from time to time.

Steve: Just kind of pull the plug. The beaches are so nice in Southern California.

Leo: I don't need to be doing this, yeah.

Steve: Yeah.

Leo: Yeah, I don't need to be doing this.

Steve: So to everybody, to the community, to the industry, wow, thank you. And to the attacker, if you want to communicate with me, I've created a line for you. I don't think you're a bad person. I think you probably wanted to play with GRC. You haven't been attacking me for days, and only two probes, short little probes, spread 48 hours apart, that I don't have any problem with, frankly. I'm asleep, and it happens, and it goes. And it's like, fine, okay.

Leo: You don't have to use Morse code, though. You can email him.

Steve: And everybody will know, if I'm forced to turn myself into a generic website, I mean, it will be a sad day. But it won't be a surprise because, I mean, I'll just tell people that I couldn't do this anymore.

Leo: I'm sorry. But I am glad you are here, and I hope you keep doing the job.

Steve: Well, that's the technology. There were a lot of people wrote with suggestions, when they thought it was just a simple DNS reflection. It's like, oh, you can filter that. And it's like, yes, but it's not just a DNS reflection, and so on. And technically, is it possible for ShieldsUP! to be on the 'Net? Well, if I had a device at a point that was larger than the attack, and I communicated with it to dynamically allow packets into this IP, the .206 IP, I think that's the ShieldsUP! IP, only from the IPs that are being tested, yeah, I mean, yes, I understand network packet flow cold. I get how all of this stuff works.

But I wrote it years ago. I'm happy to have it be available. But I just can't have it be a huge distraction for me, or I just have to kill it. So I hope I don't because a huge number of people use it. It's been around forever. And the Spoofability Test is very useful. And who knows what I'll come up with in the future. But I can't, if I have to hide behind a web proxy.

Leo: Steve Gibson, still at GRC.com. And that's where you can go to get this show, transcripts of the show, and of course all the great stuff he does there, including SpinRite, the world's best hard drive recovery and maintenance utility available for sale on the site, and the free stuff, all the free stuff, ShieldsUP! and, oh, I can go on and on and on. Perfect Paper Passwords.

Steve: Perfect Paper Passwords.

Leo: Read up on Vitamin D.

Steve: Perfect Passwords. Password Haystacks.

Leo: Tons of stuff.

Steve: Yup. The Spoofability Test and so forth.

Leo: All there, all free, at GRC.com.

Steve: All which I'm happy to do.

Leo: Yeah. You can come to TWiT.tv/sn to get copies from us, as well. We have audio and video. Best to subscribe. That way you'll get every episode automatically in your podcatcher, or use one of the TWiT apps - there's lots of them - on every platform, including Roku. There's everything. GRC.com. Don't forget, that's Steve's site. Keep it going. Thanks for joining us, and we'll see you next time.

Steve: I'm going to get back to work on SQRL, and then get it wrapped up, and on to SpinRite 6.1.

Leo: Exciting. Questions, comments, suggestions? Do not write to steveyousuck. The first time I've ever heard you give out an email address, but it's for special email. Go to GRC.com/feedback, and maybe we'll have some questions and answers next week.

Steve: I think it's time.

Leo: Yup. Thanks, Steve. We'll see you then.

Steve: Thanks, Leo.