SECURITY NOW!

Transcript of Episode #361

Paul Vixie & DNS Changer

Description: After catching up with the week's security news, Steve and Leo take a close look at the recent "DNS Changer" malware, the FBI's role in the "takedown" of the malicious servers, and the expert technical assistance provided by Paul Vixie, one of the pioneers and principal developers of the Internet's Domain Name System (DNS).

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-361.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-361-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson's here. We'll take a look at the newest Firefox, what's new; a little bit about Mountain Lion OS X and its security features; and we'll hear from Paul Vixie, the guy who practically invented DNS, talking about why his company, ISC, helped the FBI take over servers to protect people infected with DNS Changer. Paul explains all, next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 361, recorded July 18th, 2012: DNS Changer.

It's time for Security Now!, the show that protects you, your loved ones, and all you know, all about you. For privacy and security online, there's nobody better than the Explainer in Chief himself, Mr. Steve Gibson. Hello, Steve.

Steve Gibson: Hey, Leo. Great to be with you again, as always.

Leo: I was just showing Steve some fine Cabernet, sent to me by a viewer. I'll save it for you because I know you're a Cab fan.

Steve: That's my poison, yes.

Leo: Preferred poison. So today I'm really interested because I have been, and I remain so, and I'm willing to have my mind changed - somebody tweeted me because we were talking about another topic, I think it was Windows or Microsoft strategy, and I changed my mind on the air because Andy Ihnatko convinced me that Microsoft's strategy was actually good for consumers. And I said...

Steve: There is a strategy? I wasn't aware.

Leo: That was my problem. But I thought, this is a badly run company. They're telling people ahead of time that here's a new version of the Phone system, Windows Phone 8. It is going to be available sometime in the future. And any phone you buy today will not be upgradeable. That to me was like Osborne, the Osborning of Microsoft, saying don't buy it. Whatever you do, don't buy the current product because a new better one's coming, and you can't upgrade.

And he kind of convinced me that, yes, but isn't this honest, telling consumers? Apple would never do that. But really isn't it more honest to say, look, we've got something better coming along. It's bad for business. And so I changed my mind. And somebody tweeted me, saying "You're such a flip-flopper." And I really wanted to kind of say, no, it's appropriate to change your mind when presented with...

Steve: New information.

Leo: ...new information. And if there's a...

Steve: Absolutely.

Leo: So I am prepared, all of this is a long way around saying I'm prepared to change my mind on my position. But I'll restate it, that the FBI mishandled DNS Changer, that they should not have kept that DNS server running silently along until last week, that they did us all a disservice. But I guess we're going to talk about that today.

Steve: Well, yeah. What I liked was that I ran across a really nice sort of retrospective, here's what happened, by the god of DNS. And I'll set this up, after we get caught up with the week's news, by explaining a little bit more about who Paul Vixie is because he is DNS, for all intents and purposes.

Leo: He wrote BIND, which is the original DNS.

Steve: Yeah, I think like from version four point something to eight point something. So, like, 4.2 through 8.2, he was the chief officer. And what I liked about what he wrote was there were a number of useful insights that I thought would, first of all, this gives us some really great background. This was all sort of brought to the fore because I was surprised by the amount of popular press - this was weekend before last, the weekend before the Monday that these alternative servers, the DNS servers that had been sort of switched over to and commandeered and, well, we'll explain all this. But I was surprised how much of the popular press got involved, warning people that malware was going to strike on Monday. And it's like, okay...

Leo: Wait a minute. It already struck.

Steve: Way the wrong message. And so it's like, okay. And so anyway, so I saw what Paul wrote. And I thought, okay, there are so many really interesting points he makes that it's a perfect discussion for us. So that's our podcast for today. I think people are going to find it really interesting. And a bunch of interesting news.

Leo: And I'm prepared, if need be, to modify my opinion. I can't think of a single thing that would make me, but...

Steve: And this may not. It isn't my goal to do so.

Leo: Hey, but Paul Vixie says something, I listen. Right?

Steve: Yeah. I would.

Leo: If you say something, I listen. If Vixie - there are certain people you just know they know their stuff. Mr. Gibson. Let us get underway. First, Firefox 14 came out.

Steve: Yeah.

Leo: And I knew you would jump on this. This is so cool. Go ahead.

Steve: So, yeah. We're now seeing a chain of releases from the Mozilla folks. Instead of having - I know Firefox 2.0 we had for a long time, then 3 finally. Then with 4 they began to accelerate their release schedule. I did see an ex-Mozilla person, and I don't know what cross he might be bearing or what axe he has to grind, complaining, saying that this new approach that the Mozilla team has taken is lowering the quality of the product, as if they're trying to keep up with the release rate of Google's Chrome browser. From our client standpoint, from the standpoint of users, I see nice things happening. So we got 13, which then jumped to .0.1 when they fixed a couple of little release things, just recently on June 5th. So, what, six weeks later we move to 14.

Now, what 13 gave us was the ability for a new tab to show a series of most visited thumbnails, and the SPDY protocol was enabled by default. And I ought to mention that a number of people tweeted me about SPDY apparently not being as SPDY as we thought. It was one observation from sort of a grumbly old guy who seems to not be very happy with where HTTP - wait, no, not that, yeah - HTTP 2.0 is headed. There are a number of sort of converging programs, and in this posting he attacked all of them on differing reasons. And he did have specific things that he needed from HTTP that SPDY wasn't providing. And it's like, okay, well, sorry we didn't provide what you wanted.

So I just think it's good that it's there. It is the case that you can support the protocol and not get a lot of the benefits until you deeply support the protocol. That is, there really needs to be a little bit more engineering going in than just adding a few of SPDY's features. And that's certainly what Google did when they were developing it in order to get a sense for what it could really do. So it doesn't cost us anything. It's like, okay, so now it's enabled by default from Firefox 13 on. And certainly it's supported by Google's Chrome.

So now we're at 14, as of, I think, Monday it was released. It was in the beta chain for a while. And as I understand it, they've got a number of major releases sort of moving along over time. One of the headline features of 14 is that it now supports Google searches up in the - they have some funny name for it, the WonderBar or something, I can't remember what they call it.

Leo: The AwesomeBar, I think, is...

Steve: The AwesomeBar, right. It's like, okay, well, I guess that's more awesome than not having it. Anyway, they're now, since Google robustly supports HTTPS, all of the searches that it's doing for you in the AwesomeBar are SSL protected. So that's nice.

Leo: That's nice. That's actually great. I mean, it would be nice if they just turned SSL on everywhere. But I guess that's asking too much.

Steve: Right, well, you need to know that you've got it over on other side, that is, on the server side. Otherwise, attempting to SSL when not being instructed to can really slow things down. You're going to fail. You're not going to have a certificate. Then you've got to back off and so forth. Also, sort of in a bug fix-y thing, they're now offering full-screen support for Firefox under Mac OS X Lion.

Leo: Yay.

Steve: Yes, which they didn't have before, especially since you seem to have - you were just saying a second ago that you were backing away from Chrome for the moment.

Leo: I've been using Safari because Chrome is slow and buggy on Mac OS X. And so I'm trying Firefox 14. I made it my default browser today, just to see.

Steve: And then something that we have touched on since it's been in the works for a number of their major versions, it's known sometimes as "click to play" and other times as "opt-in activation for plugins." That's sort of the formal name in their developer docs. And it's at the preliminary stage now, with a release target for version 16, so a couple more obviously major releases from where we are at 14. It's disabled by default. But once again, you can go to about:config, anyone who wants to play with this.

The idea is it is giving us, for the Firefox users who really do want the sense of and the reality of more control over their web surfing experience - see, what I recognize clearly is that we're all not cut from the same cloth. There are people who just - they're not into security. They're not into the experience of using the Internet the same way probably listeners to this podcast more tend to be - those of us, for example, who are using NoScript and don't mind saying, okay, wait, this website doesn't seem to be working right, let's enable scripting and see if that fixes it, so that we're in general not surfing with scripting enabled.

Now, natively in Firefox, you'll be able to not surf with plug-ins enabled, like Flash, like Java and anything else that is an add-on to your browser, unless you selectively enable it for a page. And you are now able to do per-site enabling, so that you could say, if I have a plug-in that Google wants to run, then, fine, I'll allow Google to do it, but not if I'm randomly surfing around the web and get zapped. And in fact, we'll be talking a little bit later in this podcast about a new multiplatform trojan which has been found, which infects Windows machines, Mac machines, and Linux machines. It's an equal infecting opportunity trojan.

So there are obviously some benefits to not running with plug-ins going all the time. This is built into 14 disabled. So you go "about:config." And then, since that page is ridiculously full of settings, you want to search, just put the phrase "plugins" into the search term. Even so, you get a huge list of things. Look about two thirds of the way down, and the item you're looking for is plugins.click_to_play. It'll be set to False normally. You can just double-click it to turn it to enabled and restart Firefox and experiment with this new feature.

So anyway, I'm delighted that they're moving forward. I'm a little upset with Chrome at the moment because it really seems to be suffering from what Firefox was suffering from for quite a while, and that is it's become quite memory intensive. I mean, "bloat" is the word I'm trying to work around saying. If I launch it, it squats on about 333MB of RAM, just firing it up. I love their security model, that they have a separate process model and they're communicating cross process, that each tab is in its own process. There's a lot architecturally that I think they've done well.

I hope at some point they will, as the Mozilla folks did, realize, whoa, while we've been busy adding things, this thing has gotten really big. We need to now step back and get this under control because, I mean, it's - I have Task Manager running in Windows, and I launch Chrome, and as I said, about a third of a gig of memory is just gone, taken by it. And that's without any expensive pages loaded. So at some point I hope they are going to get that under control.

Speaking of which, they have just taken themselves, that is, Chrome, to v20. And it's 20.0.1132.57 and counting. They fixed three critical vulnerabilities. Two were "use after free" errors, where memory is released, but there's still a pointer to it which a clever hacker can use in order to exploit that fact, that dangling pointer, essentially, in order to execute code of their choosing. There is also something that they described as a "layout height tracking bug," which they called a critical vulnerability. So somehow, someone clever found a way to do that. In fact, the guy's handle is "miaubiz." He's someone who has found many bugs in the past. And I had forgotten that they have a Security Hall of Fame at Chromium.org, and they really do pay out. The top two guys who have been finding bugs have earned for themselves each $60,000 by finding...

Leo: That's not bad. You could make a living doing that.

Steve: It is. And in fact, just for these three critical vulnerabilities, this miaubiz guy, who's No. 3 in the Hall of Fame, although he's ranked there with a bunch of others who also have made $10,000, for these three he received $8,000. And I don't know whether that thousand was updated in the Hall of Fame list yet. So, yeah, there are guys there who have made $60,000, thanks to Google's paying people for finding problems. Which I think is effective for them. This also includes some stability improvements for the browser, as well as updates to the Flash Player flug-in - Flash Player plug-in.

Leo: The Plash Player flug-in? Okay.

Steve: And their JavaScript engine, V8, has also been improved. So they've continued moving it forward. And just after the podcast last week came to the news was the fact that Yahoo! lost control over 450,000 logins for their voice messaging service. And they of course learned, the way these companies do these days, unfortunately, because their customers' email addresses and plaintext passwords were posted publicly. So this tells us not only was their security not up to par - because an SQL injection was able to go in and query an SQL backend database that was available. So not only was that a problem, but what was stored in that database was plaintext passwords, no hashing being done.

So, I mean, and the way people began to see this also, and we see this also, was people began to get their accounts hacked. So the hackers stated that they posted the data to highlight the need for improved security. It's like, okay, well, good. Yahoo!'s response was, "We moved aggressively to fix the problem," which I guess is being unaggressive about fixing it. And in the news, what, I guess in the last day or two, Leo...

Leo: Yesterday, yeah, Marissa Mayer.

Steve: Yeah, Yahoo! has acquired a new president.

Leo: And that's actually very exciting. It's a daunting task.

Steve: I was going to say, don't you think it's too late?

Leo: I don't know. You know, it's so funny, technology companies, up and down, up and down, it's very volatile. And I think that having...

Steve: Yes, they could remake themselves.

Leo: That's right. Yahoo! is still a strong property, and having somebody like Marissa Mayer at the head, there's a lot to do, but I think she can bring - she's such a marquee name.

Steve: Yeah.

Leo: It's a shock, frankly. Nobody had talked about her at all, and we don't know how it happened. But I think it's the best possible scenario for Yahoo!, let's put it that way.

Steve: Yeah. So here's a really interesting scenario that I thought is also a perfect cautionary tale for our listeners. And Mark Russinovich's second book is not out yet. I've read it, and it's going to be coming out in September, he said. He has agreed to appear on the podcast. So we're going to get...

Leo: Yay.

Steve: Yes, we're going to get Mark R. on to talk about the book and the things that it talks about because I can't think of a better fun, fictional, but, boy, is it fact based, read. It reads like a novelization of many of the things we talk about on the podcast. So here is a true story that reminded me of Mark's book. And this was the - H-online.com reported this, that a number of infected USB drives were recently left in the car park of a Dutch chemical firm, DSM - and they're DSM.com - in a failed corporate espionage attempt. According to a recent report from a Dutch newspaper - and I went there, but it was in Dutch, so I didn't make very much progress there because I don't speak Dutch. But it's Dagblad de Limburger is the newspaper's name.

They said the drives were planted by an unknown party in the hopes that one or more of the company's employees would find them, pick them up, wonder what's on them, and insert them into their office computer. But this was foiled because, instead of plugging it in one of the company systems, the employee who found one of the USB sticks turned it over to that company, DSM Chemical's IT department. Upon examination, the IT department discovered that the drives contained malware that was set to automatically run upon being inserted into a computer. The malware is said to have been a keylogger designed to capture usernames and passwords and access that company's internal network to send them to an external site.

And upon finding this, the company blocked all access to the IP addresses which the malware attempted to contact because, they say, it was a clumsy attempt to steal data, and no damage was done. And of course blocking the IP addresses that the malware was attempting to connect to would prevent it from succeeding if there were other - and apparently several other USB drives were found. They went out and looked through the parking lot and found some other ones that were identical. So they were hoping that one employee would just pick them up, find one and think, huh, I wonder if there's anything tasty on these, and in the process get this thing installed inside the corporate network.

And of course we know that this is the way that Stuxnet was propagated because the internal network that was being used by the Iranian nuclear enrichment process was deliberately isolated. There were no networking connections. Yet that didn't stop it from jumping, from using a USB drive and the zero-day exploits that Stuxnet was using at the time allowed it to jump the so-called "air gap" over to those systems and wreak the havoc that it was designed to. So but this is the kind of thing going on at the corporate espionage level is let's just toss some USB drives around, and maybe we'll get lucky. And if not, we'll send targeted email or whatever it takes in order to get inside this company whose network we want to be in. So, wow.

Leo: Spear phishing.

Steve: Yeah, yeah. And I just picked up on this. I thought maybe you would have some more news about it, Leo, and that is that Mac OS X Mountain Lion, the Golden Master, was just released to developers. Apparently the rumors are it's scheduled for release on

July 25th, so pretty soon. And I was looking at it from a security angle, was there any security news that I could bring to our listeners, and all I really saw was more UI sort of things where they're continuing to move OS X and iOS closer together, mostly by moving OS X closer to the feel and features of the iOS platform.

Leo: The big change - and by the way, of course no one knows dates, but they have said, Apple has said the end of July. So it will be, without a doubt, in the next couple of weeks. And the 25th seems reasonable. They have an earnings call on the 24th. Last time they announced that Lion would be available the day after the earnings call, which this time would be the 25th.

Steve: And I did hear that there was some employee announcement that went out saying plan to work late on the 24th.

Leo: Those are pretty much useless.

Steve: Okay.

Leo: Take it as a veteran Apple watcher. Because they do overnights all the time. But there is a thing, and I would love for you at some point to look at it, there is a security feature that is significant in Mountain Lion. It's called Gatekeeper.

Steve: Okay.

Leo: And there's a couple of very big changes. But the key to Gatekeeper is that from now on you will have a setting on all OS X devices that controls what's installed. So it's going to be a little bit like iOS or Android. And by default you'll only be able to install from the Mac App Store. You have a box that says "Mac App Store" and "Identify Developers." And Apple will have a certificate situation, a public key crypto certificate, identifying developers; or the least secure, of course, the way it is now, you could download anything, anytime, anywhere.

Steve: Free for all.

Leo: Free for all. So these - I think this is really great. I'm not sure what the default setting is. The way it's marked on their Apple website is the middle setting, which is actually probably what most people will want, which is either buy it from the Mac App Store or by a developer with a certificate. So malware, of course, unless they can figure out a way to hack the certificate situation, will never have a real identity. So I think Gatekeeper is going to be a significant security feature. And they are now requiring developers who want either to be in the App Store or a certificate to identify ahead of time what kinds of access to the operating system they want. They'll be sandboxing. And if you do not identify - you won't have - for instance, let's say you want to have access to the file system.

Steve: Yes, this is major changes. And we've talked about the sandboxing in OS X before, and so they must be moving it forward.

Leo: In effect they're going to kind of somewhat require it. You'll have a choice. They're also, let's see, I think that they are adding address randomization. I don't know if they had that before, but they certainly will have it now the address space, data space randomization.

Steve: Yes, ASLR. What I remember was that it was not as robust as it could be, and that they were going to be increasing it to make it more useful somehow.

Leo: My suspicion is that this will be the beginning of that. And then they are adding to the privacy controls. So as you know, the Do Not Track setting will be added to Safari, not by default on, but it will be there. And you can limit or block cookies and limit website access to location services. I think they're going to have a built-in password generation assistant. They've always had that, but it's been hidden in the Keychain. Now it'll be much more public.

Steve: And I think it's, like, $20, right, to upgrade?

Leo: It's $20. Almost everybody will do it. That's the way it is in the Apple world. People tend to do upgrades more so than in the Windows world. And it's an App Store update. So you just go to the App Store, you download it, and it installs.

Steve: Oh, nice.

Leo: Yeah. So I think this is a major move toward security. There's underlying stuff that Apple doesn't talk about, antimalware stuff that Apple doesn't talk about much in OS X. And I suspect that will also be beefed up. So, yes, I think there are actually some significant security implications to the new one.

Steve: Cool. So F-Secure, the well-known security company that we refer to every so often when they come up with something interesting, discovered a cross-platform Java trojan. It's the first one that we know of which runs on all three major platforms. There have been some Mac and Win cross-platform malware. This one now brings UNIX and Linux into the fold. And they show in their posting the source code or the Java code for this, where it uses the system objects getProperty and gets the os.name, changes it to lowercase, and then it checks to see if that contains the string "win." If so, it customizes some code and installs the Windows-specific malware. If not, it checks that string to see if it contains the substring "mac." If so, it installs the Macintosh variant of the malware.

Leo: Wow. That's pretty sophisticated.

Steve: Otherwise, it checks to see whether that os.name either contains an "nix" or an "nux." And if it's either of those, it installs the Linux/UNIX malware. So they called it

Trojan Downloader:Java/GetShell.A for the Java component. And then either W32, OSX, or Linux/GetShell.A for the three different versions. And interestingly, the OS X is a PowerPC binary.

Leo: They couldn't be bothered to update it, for crying out loud? That's ancient history.

Steve: So you have to have Rosetta installed on an Intel platform in order...

Leo: Rosetta does not come with Macs anymore. So either they're intentionally targeting old systems...

Steve: And creaky.

Leo: ...or they don't know what they're - maybe they just don't know how to update the code.

Steve: Yeah. Odd.

Leo: That's weird.

Steve: Very odd. And when you get infected by this multi-headed Hydra, it connects to a Command & Control server and awaits further instructions. And that's typically downloading and executing additional malware. They have been monitoring the Command & Control server with their own honeypot install, and so far no instructions have been forthcoming. But maybe the bad guys are waiting to acquire a critical mass before they start using it.

And then we also had a Dropbox Spam and Outage event in the last couple days. European Dropbox users began receiving gambling casino spam to email accounts which they only used and set up just for Dropbox accounts, which was of course the canary in the coal mine that, oops, somehow email accounts got loose from Dropbox. And the last posting I saw from Dropbox was at 3:37 p.m. Pacific time yesterday, where they said - oh, and I should mention that there was also an outage, about 30 minutes, where Dropbox stopped working. We don't know if it was Dropbox taking themselves offline in order to fix the source of the security problem, or I also heard reports that it was some sort of denial of service attack against Dropbox.

So at this point things are a little bit muddy because this has just happened. But the Dropbox PR face said, "We're aware that some Dropbox users have been receiving spam to email addresses associated with their Dropbox accounts. Our top priority is investigating this issue thoroughly and updating you as soon as we can. We know it's frustrating not to get an update with more details sooner, but please bear with us as our investigation continues." And I want to thank Brian Krebs, who was my source for this information. He was on top of it and tracking it down.

And while I'm thanking people, I want to thank Daniel, who is in Bedfordshire, England.

He said, "Hi, Steve, Leo. I've been listening to you guys since the first episode and want to thank you and Leo for making my journey to work so much more enjoyable. I bought a copy of SpinRite many years ago in support of your podcast, but never had the opportunity to use it. Well, it finally happened. My hard disk failed. And rather than worry about data loss," and he said in parens, "(fortunately I use Carbonite)," he said, "I immediately went looking for my copy of SpinRite. I popped it in, and two hours later I was up and running again. So yet another hard drive saved. Thank you for a wonderful podcast and building an HDD recovery tool that does what it says on the tin for a very affordable price."

Leo: Does it come in a tin?

Steve: Eh, no.

Leo: I like the idea, though. You might want to put it in a tin.

Steve: I love the jargon. And then in Bedfordshire, England-ese, he says, "Keep calm and carry on. Best regards, Daniel."

Leo: Isn't that great.

Steve: Daniel, thanks for the report.

Leo: All right. Back we go to the task at hand, Mr. Steve Gibson.

Steve: You know, I did realize, I was thinking about commuting, and it is now the case that the standard image you see of any sort of gym club environment is everybody with things in their ears as they're on their treadmill or doing their machines. We don't know if they're listening to music, but could also be audible podcasts.

Leo: I really like listening to books because you don't have enough time in the world to read, frankly. And so that hour a day that I work out, that's an hour a day of extra reading. I think that's really, really nice.

Steve: Okay. So who is Paul Vixie? I pulled together some sort of interesting and fun bio stuff because I wanted to give our listeners a sense for who this was who wrote what I will then read. So he's got his Ph.D. - I put "Ph.D. in DNS."

Leo: [Laughing] It's true.

Steve: But he is Dr. Paul Vixie. He's currently the chairman and founder of Internet Systems Consortium, ISC, who Internet-savvy people know is the publisher and maintainer of BIND.

Leo: And, by the way, the people who ran the FBI server for them.

Steve: Yes, exactly. And I said, as I was researching this, I said, I note that Paul was also previously president of ISC in addition to chairman and founder because I found this dated January 15th of 2011. He says, in quotes, "'I am relieved.' That lovely double entendre is what Captain Pike said to Captain Kirk..."

Leo: [Laughing] That is nerdy.

Steve: Uh-huh, "...at the end of last summer's most excellent reboot of the Star Trek series. I am likewise...." And you remember, like, Pike was in his wheelchair at that time. And he said, "I am relieved." He said, "I am likewise relieved to have been relieved of my long-time post as president of ISC by my good friend and long associate Barry Greene. I continue at ISC as Chairman and Chief Scientist, which is the equivalent, to me, of escaping to the candy factory. When ISC was smaller, this was the half of my job I loved most." So this is Paul's way of saying I love the technology; but I was president for a while, and, boy, am I glad that I get to hand that off now so I can just get to play with the technology again.

So he was the principal author, as I mentioned before, of BIND from versions - he took it up at version 4.9 and carried it through 8.2. And I'm sure most of our listeners know that it is the leading DNS server software in use today. There are other server companies. For example OpenDNS famously uses their own. Microsoft got into the game late. But the big DNS servers, the big iron DNS servers, they're universally running BIND. It is, like, it's the gold standard.

Paul was the principle author of the DNS RFCs. He did RFC 1996, which is the DNS NOTIFY RFC, which provides a means for a DNS server to notify one that is authoritative to it that it's got changes in its records; RFC 2136, which is the DNS UPDATE spec; RFC 2671, which is eDNS/rDNS extension fields and how they're handled. And he coauthored 1876, which is DNS LOC; 2317, which is DNS for CIDR, where you don't just have networks that are A, B, and C class, but you have flexible masking so you can sort of tune networks to whatever size you want; and RFC 2845 for DNS TIG.

So, I mean, he's really been into it. And I found another little thing written about him that says he served as president of MAPS, PAIX, and MIBH; as CTO of Abovenet/MFN; and on the board of several for-profit and nonprofit companies. He's served on the ARIN Board of Trustees since 2005, where he served as chairman in '08 and '09, and is a founding member of ICANN, the Root Server System Advisory Committee (RSSAC) and ICANN Security and Stability Advisory Committee (SSAC).

"Vixie has been contributing to Internet protocols and UNIX systems as a protocol designer and software architect since 1980," so, what 32 years. "He is considered the primary author and technical architect of BIND 8," which was, for those who don't know, a major rewrite to bring it current. And the open source projects do, if they have a really long history, they tend to get a little crufty over time. And so every so often you have to just say, okay, wait a minute, we're going to take everything we've learned, and we're just going to start again. And so it was time to do a major rewrite of the server platform. And he hired many of the people who wrote BIND 9 and the people now working on BIND 10. So he's really steering the future of DNS on the Internet.

And then, in something completely different, but I just thought this observation was interesting, I found where he had written something sort of sad, but it demonstrates that he does have his finger on the pulse. He wrote, "Most new domain names are malicious." He said, "I am stunned by the simplicity and truth of that observation: Most new domain names are malicious. Every day lots of new names are added to the global DNS, and most of them belong to scammers, spammers, e-criminals, and speculators. The DNS industry has a lot of highly capable and competitive registrars and registries that have made it possible to reserve or create a new name in seconds, and to create millions of them per day. Domains are cheap; domains are plentiful; and, as a result, most of them are dreck or worse." Which is sort of a sad statement. But, unfortunately, this is what happens as something like this evolves and matures.

So on March 27th, Paul wrote of his experience with DNS Changer. He said, "Takedown: One fine night in November 2011 I got an opportunity to get my hands dirty, working on a project for the United States Federal Bureau of Investigation (FBI). They were planning to seize a bunch of computing assets in New York City that were being used as part of a criminal empire that we called 'DNS Changer,' since that was the name of the software this gang used to infect half a million or so computers. I work for Internet Systems Consortium (ISC), a small, non-profit company headquartered in California. ISC is best known for our work on the Domain Name System (DNS) and our DNS software called BIND, but we have a growing Internet security practice, as well.

"My task that night in New York City was to install two replacement DNS servers supplied and operated by ISC. This was important because the victims of DNS Changer were dependent on the assets that the FBI needed for evidence, and none of us wanted a half million DNS Changer victims to go dark. It was a little odd for ISC to send me ISC's chairman and founder on this job, but rank hath its privileges. It was a very long night, since there was no way to complete a detailed plan before the takedown began. After the DNS Changer gang was in custody and I could 'go intrusive' on their equipment, it took me a couple of hours to figure out exactly how everything was wired together."

And of course I should say that by that he means he's just seeing some stuff running, but obviously he knows everything there is to know about the subject matter. But it's always the case when you're approaching something like this, it's like, okay, how, down at the lowest level of detail, have they done this? What ports are they using, what relocators, what routers, what proxies, I mean, you need to really understand it.

So he says, "It took me a couple of hours to figure out exactly how everything was wired together and to move the first group of victims over to ISC's replacement DNS servers. It then took a couple more hours to move and test the rest of the victims. All this long night I had a cell phone headset in one ear and a half dozen chat windows open on my laptop. The full takedown team was worldwide, and there were other actions occurring elsewhere. By the time we were done, and it was safe to power off the DNS Changer equipment, it was 7:00 a.m., and I nearly missed my train. Note to self: If another chance comes along to run huffing and puffing through the New York City subway system and Penn Station, trying to keep up with a younger and better conditioned member of FBI's New York division, take it, but maybe next time bring better shoes."

So about cleanup he says, "Since the original court order that authorized ISC to install and operate these replacement DNS servers was due to expire on March 9, 2012, a new DNS Changer Working Group (DCWG) was formed to handle victim notification and remediation. We had roughly four months to identify and notify half million or so DNS Changer victims, and to help these victims clean up their infected computers. Many victims would have to reinstall Windows on their computers, which at first was the only sure cure for this particular infection.

"On top of that, many of the victims have had their DSL or cable modems - their home routers - reconfigured by the DNS Changer malware" - so that's one point we want to talk about is, as we know, this stuff was able to access their routers and change the settings there - "so that they were using ISC's replacement DNS servers, even if none of their computers are still infected, and even if none of their computers were running Windows. Most Internet users do not have the skills necessary to check and repair the configuration of their home routers, and most Windows users are also unwilling to reinstall Windows. So even when we could identify and notify a victim, we had a hard time closing the deal.

"We didn't make it. When March 9, 2012 loomed, we still had hundreds of thousands of victims dependent upon ISC's replacement DNS servers. Therefore, the FBI asked the judge for an extension, and we were given four more months. No fooling around this time. There won't be another extension. It's now or never. Put up or shut up, et cetera. Noting that no private company or individual can legally operate this replacement DNS service on the open Internet unless they have a judge's permission to do so, many ISPs are now starting up replacement DNS servers inside their own networks, accessible only by their own customers, in order to control the risks that they would otherwise face on July 9, 2012, when the second and final court order is due to expire.

"But that kind of risk management isn't the same as cleaning up the problem. I don't think we want to kick this can down the road. If an ISP wants to run a replacement DNS server for the purpose of forcibly breaking these computers in small batches, to get their owners to call in and then ask for help, that's one thing. But it's just going to be a new permanent service that the ISP offers these customers" - oh, I'm sorry. He says, "But if it's just going to be a new permanent service that the ISP offers to these customers, count me as opposed. We as a digital society...." And here's one of the things that I really loved about what he wrote: "We as a digital society are much better at strategies for coping than we are at strategies for remediation." Which is to say, for fixing.

"Is your DNS okay? A half dozen Internet security teams around the world have created special websites that will display a warning message to potential victims of the DNS Changer infection. For example, if you visit http://dns-ok.de, you'll get a German language page saying either that you appear to be infected or that you appear not to be infected. Andrew Fried and I created dns-ok.us" - which I mentioned to our listeners a week or two ago - "for the same purpose," he says, "though of course our page is in American English. The full list of these DNS-checking websites is published on the DCWG's website, along with a lot of information about the threat, the arrests, the takedown, the court orders, and clean-up information for victims.

"Now that we've got all these websites that are able to tell someone if they're a victim and that tell victims what to do to clean up their computers and their home routers, the problem seems to be getting people to care." Meaning people still aren't caring. "Internet users are endlessly bombarded with warnings about their security and with offers of services and software, some of it apparently free, offering to make their computers healthier. The victims of DNS Changer are by this time jaded or overwhelmed or both. The Internet seems to be a very dangerous place, and most Internet users probably feel that they could spend more than half their waking hours just installing patches and responding to warnings, unless they just put their heads down, ignore all that noise, and try instead to get their work, or play, done.

"I'm sympathetic to this mindset," says Paul. "The problem is, the Internet really is that dangerous, and people really do need to pay more attention to the dangers of unpatched or infected computers. Given that most people can't take the time to care enough about these dangers, their infected computers become a threat to everybody else, thus completing the cycle of dangerousness begetting more dangerousness. All those within the sound of my voice, please check out the DCWG website and find out if your DNS is okay. Ask your customers, your friends, and your family to do likewise. Or use this as an excuse to go visit the people in your life less technical than yourself and show them how to check their DNS."

And so, wrapping up under, he says, "July 9 and Beyond: On July 9, 2012 the replacement DNS servers operated by ISC will be shut down" - remember he was writing this on March 27. So they "will be shut down, and any victims who still depend upon these servers will face new risks. Notice I'm not saying that they will go dark, since that's not entirely clear. Some of them will go dark; some of them will face long delays on every web page they visit; some might not show any symptoms at all. The long-term risk I foresee is that some new criminal empire, or more than one, will offer services to again replace ISC's, and they will easily recapture a large part of the DNS Changer victim population. There are ways to do this that don't leave tracks, so not every criminal who does this will be automatically and immediately detected, arrested, and charged. I would like to see these computers cleaned up so they don't pose a lasting but latent threat to the rest of us.

"Speaking of lasting, latent threats to the rest of us, I was part of the Conficker cabal recently immortalized by Mark Bowden's book, 'Worm.' We still don't know the identities of any of the criminals who foisted Conficker on an unready world back in 2008, but we do know that the victim population has not dropped below six million. So we still collect the sinkhole data about these victims; we still report on it to network operators; and every year we buy another rack of disk drives to hold the next year or so worth of data. We're out of ideas for how to get people to care that their computers are infected with Conficker. These victims seem to feel that they have more important things to worry about. My gut feeling is that they're wrong, but I can't seem to prove it. My other gut feeling about all this is that we, as a digital society, are doing this all wrong. Paul Vixie."

Leo: Hmm.

Steve: So there's a lot of things to think about there, Leo.

Leo: Absolutely. Absolutely. I still think they did the wrong thing, but that's...

Steve: What's interesting, I was working with Jenny, setting up a new laptop for her. Hers was just getting old, and I wanted to get her set up with a new one. And so we were sort of inventorying her existing one. I wanted to, in setting it up, not reinstall things she didn't use any longer. And it's funny because we were sitting side by side, and dialogue boxes were popping up which she was - her immediate instinct was to close them. Say "Okay." And it was educational for me because I read these things. I know that there's something that I'm being told, and I wanted to know what it was. But Jenny is not a computer person. She just wants to write her novels and screenplays and, as Paul says, get on with her life. And so this is all just intrusive for her. And she sees it as something she clicks "Okay" to, in order to just get on with what she's doing. Which I'm sure she's representative of the majority of PC users.

As Paul writes, somehow we haven't done a good job of this. Somehow we have - and again, the listeners of this podcast are with you and me, Leo. But they represent the people, the broader, I mean, this narrower audience, this group who are the influencers of - they're the people whose voice has been reached by Paul and through this podcast. And they're the tech support for their families and their neighbors and their coworkers. And doubtless they see this as you and I do, that there's something not right about, unfortunately, about the way this is working.

And I thought these numbers were very sobering, that despite months of DNS being misconfigured, they were never able to get the last third of these systems fixed, no matter how hard they tried. And here's six million machines infected with Conficker. And anybody who puts a packet sniffer out on the 'Net is getting pinged by Code Red and Nimda. They're still out there, scanning the 'Net, trying to infect machines. And I coined the term, as you know, a decade ago, IBR, Internet Background Radiation. That's what this stuff is. It's become part of the ecosystem on the Internet. And it is sad that we've sort of abused the users who just want to get their work done.

Leo: You know, I detect a little hint of a kind of common paternalism that you hear from old geeks.

Steve: [Laughing] Yeah?

Leo: And a little bit of blaming the user. It's their fault. And I think really he should take more blame for setting up a system that doesn't work and should be putting more effort into fixing it than blaming the user, to be honest. And there's a lot of old-time geeks who say, well, if we could just get people to - he says something, the most important paragraph to me in here is he says, "If an ISP wants to run a replacement DNS server for the purpose of forcibly breaking these computers in small batches to get their owners to call in and ask for help, that's fine. But if it's just going to be a new permanent service that the ISP offers to these customers, count me as opposed."

But that's exactly what he did for seven months. I no longer blame the FBI. I think it was a little misguided on Paul's part. But we could debate that. I think the point that he makes that's interesting, that I hadn't really thought about, is had they just pulled down those servers, there's the risk, and there's the risk now, that some malicious entity would just recreate a server at that address.

Steve: Yes, recapture, exactly. And the other thing he made clear that wasn't obvious to me is that only by permission of a court could they operate servers at those addresses. And the point about the ISP is that an ISP can control their network. The ISP's network is not the public Internet.

Leo: And they can see outbound traffic to that DNS server.

Steve: Exactly. So they could set up some filtering on their routers to route those malicious DNS IP queries to their own DNS servers and provide valid service to their customers. And also notice that the ISP does know who those people are because they're getting - every DNS query comes from an IP that the ISP controls. And so, one by one, they could log them and send them email. They have their email address. Send them postal mail. They're probably charging them, so put a big red pink slip...

Leo: Fix it or else.

Steve: ...in their bill. It's like, okay, call us, please call us. Your machine may still be infected. And in any event, it's still misconfigured.

Leo: Nobody wants to do that because the amount of support that's required to fix it is so expensive that no ISP wants to assume that mantle. I can promise you. Look at Comcast, how many millions, tens of millions of users do they have? They're the biggest ISP in the country. They start doing that, they're responsible somehow for fixing millions of computers? Whoo. Fortunately...

Steve: Yeah. It does creep me out, though, I mean, just the idea that in every ISP would be a DNS server or some filters, like permanently stuck in a router...

Leo: It's just a redirect. It's just a redirect. It's a router saying, hey, if they go to this address, send them here. It's not a hard thing to do. The problem I have with doing that is the same problem that Vixie has. You cannot keep these infected machines online. You have to do something. My opinion is the best thing to do would have just been break it right upfront. So what if there's a howl of protest? Those people need to know immediately that they're infected so that they can take action.

Steve: So the idea would be that they would get a court order to so-called "blackhole" that IP. That is, they would not offer DNS services, but they would just acquire the IP and just, like, have the machines go dead. And then the users would say, oh, crap.

Leo: Something's wrong.

Steve: Something's wrong.

Leo: And then they would - some of them would call their ISP. Most of them would bring it into the shop or call me on the radio show...

Steve: I wonder if...

Leo: ...and we'd tell them what to do. The problem is those people for seven months have been running infected machines. And as you know, the chances that they have more than one infection are high.

Steve: Yeah. I wonder if there are some unappreciated consequences, unappreciated by you and me, of doing that. See, we only think in terms of...

Leo: I know.

Steve: Like what if their household alarm system is Internet based, or their...

Leo: But the damage was done when they were infected by DNS Changer. I think for Vixie, for ISC, or for the FBI to assume responsibility at that point - there's also, and I think this is really interesting, the notion that somebody might hijack that IP address. Now, I wonder, if you get the court order, and you take the IP address, and you blackhole it, that kind of protects you, doesn't it? I mean, they do control DNS.

Steve: So I don't know what the IP was or who actually owns the IP. But it must be that it was a foreign IP. And so what they needed was they needed a court order in order, essentially, to break that part of the Internet, to say we're not going to allow people who are trying to get to that IP, that valid IP owned by somebody else, we're going to filter that. We're going to block that and keep people from getting there. And so the judge said, okay, but you can't do that forever. How long do you need? And they said six months ought to do it. And it turns out - or four months, I guess it was initially. And it's like, oops, that wasn't enough time.

Leo: So they went eight months. The interesting thing is, and maybe this proves that their strategy worked, we didn't hear a lot of howls of my Internet's down.

Steve: None, none.

Leo: So maybe that seven months was useful in getting people to fix it.

Steve: Or maybe the bad guys jumped in that quickly.

Leo: Whoo, that's a scary thought.

Steve: Yeah. So...

Leo: Now, correct me if I'm wrong, but if, I mean, look, doesn't ICANN control the DNS servers? Can't they say, look, no one will ever have this IP address?

Steve: No. It's that they're blocks of IPs. And so this is some block of IPs owned by somebody.

[Talking simultaneously]

Leo: Probably somebody in Estonia.

Steve: Yeah, it's that kind of thing. And so it's like a valid - all over the Internet there are routers that are routing that block of IPs to somewhere. And so...

Leo: That's right, you can't block an IP unless you block it on all routers.

Steve: Right. And so, I mean, this was a major event in terms of intercepting a couple specific IPs and saying, nope, we're going to send them over here.

Leo: No, I can see the puzzle, and I can see the challenge, and I'm sure that people have thought a lot longer and harder than I have about this and decided this was the right thing to do.

Steve: Yeah, see, I'm wondering if the trick here, Leo, is that we're not appreciating the depth...

Leo: Yeah, of consequences, yeah.

Steve: Yes, that it's more than just people not being able to log into their Facebook games or something, that taking DNS down for organizations would be, like, a big problem, mission-critical sort of stuff. On the other hand, you really don't want to be referencing evil DNS servers.

Leo: No.

Steve: That certainly has a set of consequences.

Leo: Or continue to operate without knowing that you're operating an infected machine. I think they had a responsibility to let people know that there was something wrong.

Steve: Yeah, I'm hoping that dns-ok.us still functions.

Leo: No, it does not.

Steve: Ah. That's unfortunate.

Leo: I'm not sure why it does not. That seems odd. If you go to dns-ok.us it says, "This site can no longer determine if your system is infected."

Steve: Yeah, okay, well, now, the reason is that the way it was working was, as we said when we were talking about Google, is that they know that their server picked up your query, and in this case they're no longer running the servers.

Leo: Yeah. Somebody, Scott Mishoe [ph] is suggesting in the chatroom, and this is certainly one of the things that I would have at least investigated, maybe they decided this couldn't be done, is to serve up the Internet in an iframe and all around that frame say "Warning, warning, warning, you have a virus." The problem is we have trained users to ignore that kind of thing.

Steve: Yeah, and that requires content filtering, too. So that's a step further.

Leo: They didn't want to get in that deal, did they.

Steve: Yeah. And you can't do that for SSL. It's impossible to intercept that. So there would be a lot of limitations for that approach. Anyone who's interested, DCWG.org is up. That's the URL that Paul references here as what to do from now on. And so there is a detect and fix and protect item there. And so DCWG.org.

Leo: It's the DNS Changer Working Group, is what that acronym is.

Steve: Yes, yes. And more information there. And, ooh, there's an interesting word map. Shadow server has pulled together a word map based on country to illustrate which countries - oop, it just changed. It's running some Flash...

Leo: Yeah, but it's a tag cloud of which countries are most infected. It's kind of interesting.

Steve: Yeah.

Leo: However, and I think this is a symptom of, see, I think that the problem is that these engineers don't really understand users. For instance, if you click the Detect button, it sends you to dns-ok.us, which can no longer detect. So they didn't bother to update this page.

Steve: Yeah. Wow, the United States is the biggest tag by far.

Leo: Yeah, but it was still 70,000 out of 300,000. It wasn't a majority. It was a plurality. If you go to the Fix page, yeah, it's okay.

Steve: Wow, it's not very friendly. They don't have...

Leo: Yeah. I think that these guys, we need to - the sad thing is the engineers who understand this do not understand users. And the users don't understand the engineers. So there's a real impedance mismatch here. That's the real problem.

Steve: [Laughing] I love that. That's a great term for it.

Leo: The tracks just don't meet in the middle. So I don't know exactly what the solution is. I would say, if I were Paul Vixie and company, I would take this as a huge wakeup call because they don't want to have to ever do this again. And they need to figure out what's broken and fix it.

Steve: Well, everything's broken.

Leo: That's the problem, isn't it. It's an intransigent problem.

Steve: Really.

Leo: Really is tough.

Steve: I mean, when my mom is typing "http://," that tells you something, this system was never designed for the applications it is seeing. We're just sort of limping forward. And as he says, "We as a digital society are much better at strategies for coping than we are at strategies for remediation." And it's interesting, while I was also doing the research, I ran across some other comments about IPv6. And one of the problems it's had is it doesn't really do anything that anyone is really sure they need. I mean, it doesn't offer, like, tremendously better benefits. It's like, yeah, well, we should be moving to it. Okay, but no one's in a big hurry to do that because everything's fine with IPv4.

Leo: Right.

Steve: Whereas, when something comes along like SSH, overnight it replaced all the insecure alternatives to that because everyone said, wow, this is much better. So a protocol that really - oh, I think this is in regard to SPDY, and it was the guy grumbling about HTTP 2.0 and when are we going to get that and what's it going to do? He used SSH as an example of a protocol that really did offer benefit; and, wow, it got adopted. And here, HTTP 1.1 seems to be good enough, and we're not sure where to go from there.

Leo: Well, I think that's why it comes down to operating system manufacturers making locked-down operating systems so malware has a harder time getting on them.

Steve: These are all good, incremental movements, yes, and the SSL Everywhere, Google switching to HTTPS...

Leo: Routers that are locked down a little better.

Steve: Yes, and options like No Not Track that allow users to just sort of express a preference, which is, I mean, this is all new technology. This is the way we'll get there is a little bit at a time. And as things get old enough, we can finally let them go. I mean, that's always been Microsoft's strategy is they keep the old stuff alive for a long time. And we just lost compatibility with 16-bit code.

Leo: And that's the problem is this stuff is starting to get antiquated, and it's falling apart, and it's going to get worse and worse. And you can't just pull out, pull the rug. And I think what really this ISC thing is saying is, look, you can't pull the rug out. You've got to fix it before you pull the rug out. And so we wanted the eight months to try to fix things.

Steve: I think I may have mentioned that my buddy and yours, Mark Thompson, when he switched to Windows 7, he was stunned to see how much 16-bit code he was still using.

Leo: Still running, wow.

Steve: Because he was just, I mean, it's one of the reasons I'm staying is I'm using Brief, which is a 16-bit...

Leo: Brief, you're kidding me. That's DOS program.

Steve: Hey, I can wave my BlackBerry in front of the camera, Leo, and you'll see I'm really a dinosaur.

Leo: Gibson uses DOS. Steve Gibson does this show every Wednesday, 11:00 a.m. Pacific, 2:00 p.m. Eastern time. That's 1800 UTC. Watch live. The chatroom and I talk back and forth, and it's a good way to kind of be part of the show. But of course we make on-demand versions available always after the fact, both audio and video. In fact, Steve has an unusual version that only this show has. Two things, really. He has a 16Kb audio version for really small downloads.

Steve: One quarter the size.

Leo: And, yeah, and transcriptions, which are great if you like to read along. He also has a lot of other stuff, including SpinRite, the world's best hard drive maintenance utility, right there at GRC.com. You must go there and get it. You can follow him on the Twitter, @SGgrc. And we make the larger files, audio and video, available at

TWiT.tv/sn for Security Now!. Or go to iTunes and subscribe.

Steve: Next week, Episode 362 will be a Q&A. So GRC.com/feedback. Send your thoughts, your questions, your comments, whatever you want. I will go through the mailbag, and we'll select a bunch and discuss them next week.

Leo: GRC.com/feedback. Thanks, Steve.

Steve: Thanks, Leo.

Leo: Have a great week. We'll see you next time on Security Now!.

Steve: Right-o.