SECURITY NOW!

Transcript of Episode #149

ISP Betrayal

Description: In this first of two episodes, Steve and Leo discuss the disturbing new trend of Internet Service Providers (ISPs) allowing the installation of customer-spying hardware into their networks for the purpose of profiling their customers' behavior and selling this information to third-party marketers.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-149.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-149-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

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

This is Security Now! with Steve Gibson, Episode 149 for June 19, 2008: ISP Privacy. This show and the entire TWiT broadcast network is brought to you by donations from listeners like you. Thanks.

It's time for Security Now!, time to talk about saving yourself, saving your computer, saving your personal identity. Mr. Steve Gibson is our savior - well, that's a little sacrilegious. But he's certainly the guy who's protecting us online. Hi, Steve.

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

Leo: You're my savior, Steve.

Steve: Yeah, well, I'm glad that we're doing the podcast. It's a lot of fun, and we're closing in on the end of our third year, which is...

Leo: That's neat. That'll be soon, I guess, since we've done one a week.

Steve: Well, it will be, actually, because we're doing 149 this week. And so given 52 weeks a year, which is pretty much standard, 156 will be the end of our third year. So, yeah.

Leo: That's really great. And we should say for those of you who wanted to see Steve at his fortress of security, we are now, well, we can see Steve on TWiT Live. You can join us as we record the show. We do it every Tuesday at 11:00 a.m. Pacific time, that's 2:00 p.m. Eastern, 18:00 UTC. But I should warn you, there's no clues. The entire background that Steve's got there is completely imaginary. He's on a...

Steve: Matted in on a green screen.

Leo: Because you can't deduce anything. It's not really his face. He's using that Logitech software to put another person's face on there. It's still anonymous. You were concerned, you were a little concerned about having cameras on.

Steve: Yeah, I just decided, well, I just haven't figured out how I could stick the camera - essentially this camera is sandwiched in between two LCDs. I've got a lower one and an upper one, with the camera right here in the middle. And I actually chose, one of the reasons I chose the Logitech was that it has a very thin profile so it can sort of sneak out from in between the two screens.

Leo: Wow. So how many screens do you sit and stare at?

Steve: Five. I have five here. I was thinking I ought to get a mirror.

Leo: I'd love to see it. Sometime just [indiscernible] a hand mirror. We'd just love to see that setup.

Steve: I think it was Dick who did that. It's like, yeah, here's a mirror so you can all see.

Leo: Yeah. I would love - I would really think that's very funny. I would love to see what that looks like. And that's just how you work day in, day out, huh?

Steve: Yeah, it's just I've gotten spoiled. I used to have three SGI monitors. And then I sort of changed things around. I decided it was time to get more real estate. And after you get used to it, I just, like, I have thing and - it's funny because Mark Thompson and I were talking about the way we work with multiple monitors. And he's the same way. You know, I've always got Windows Explorer open on the right side of my right-most screen. And I've got a couple browsers, Firefox and Opera at the moment, open on my left screen. My [indiscernible] of course [indiscernible] working area. But so everything is in a place. I've got the stopwatch right above the camera so I can see it. And so everything's sort of - and so you just get used to this notion of not having things overlap. It makes me think also, remember Windows 1, where Gates was arguing against overlapping windows?

Leo: Right.

Steve: And the first version of Windows, I mean, it did not have overlapping windows. There was no provision for overlapping windows. You had dialogue boxes. But all the windows were tiled, and you could sort of, you know, drag their edges around. I don't know if that was to avoid copying Xerox too directly, or Apple, or what the story was.

Leo: No, in fact there was a big debate even at Xerox, and I think at Apple, too, over whether windows should be tiled. And it was a big academic debate between the two different factions. So I think a lot of the early Xerox stuff did not have overlapping windows. That wasn't technically difficult, it's just...

Steve: And the idea being, of course, it's like, well, wait a minute, if there's information being shown, then you'd see it. Why would you want to hide it behind something else? And the idea is, well, it's the concept of these things that we just now take for granted.

Leo: Well, and the right side won, I must say, because if it weren't for tiling, I mean, if it were all tiled - do they even have that command? They had that command for a long time in Windows, you could tile the windows. I don't even know if they still have that command.

Steve: It's around for, definitely for child windows, I know that you're able to, like, arrange those, so.

Leo: Right. Hey, you know, today - we're recording on Tuesday, it's Firefox 3 download day. And Firefox, nutty Firefox thought, oh, we'll see if we can get a Guinness Book of World Records record for the most downloads in one day. So they got everybody to pledge to download Firefox. And as we speak, SpreadFirefox.com, which is the locus for all of this download day 2008, is down. They couldn't plan, I guess they couldn't buy enough bandwidth. I mean, they must have known. They were saying let's break a record.

Steve: And so they slashdotted themselves.

Leo: They slash...

Steve: I have to say that I'm responsible for several features in Firefox 3. They returned the checkbox to easily disable third-party cookies.

Leo: Yes.

Steve: As a consequence of my work. GRC is in the process of producing some new technology which will preemptively inform everyone who comes to our site if they have third-party cookies enabled and essentially give them a little banner at the top of the screen to say, hey, just want to let you know that you're making it very easy to be tracked across the Internet. Click this in order to get instructions on how to change that. And the Firefox 3 guys recognized that this would generate so much interest in how do I disable third-party cookies that they decided to put that checkbox back that they mysteriously took out in v2 under the feeling that, well, it's not perfect protection, so we shouldn't have it in at all.

Leo: Well, I remember, didn't you ask them, and they said, well, it doesn't work, so that's why we took it out. It never was working anyway.

Steve: I guess that's, you know, that's a way they could look at it. But remember - and remember it was still there. You had to go to - you had to put in the address bar site:options. And then you'd get this overwhelming list of stuff. And then you'd type in COO into the search bar, and it would give you a list of about eight items that you could configure. Then you had to change one of them to, like, a 1 or a 2 or something. Anyway, they fixed all that. And they had bugs in - Firefox 3 had bugs in their third-party, well, overall cookie handling that Firefox 2 still has. So it's, for example, not possible to block third-party cookies correctly under version [indiscernible]. So Firefox 3 looks like it's going to be a good thing for people to move to.

Leo: Yeah. And then Flock, which is a Firefox derivative that I use, is also updated to Beta 1 of v2. And it has the same security features, many of the same security features, but does not have the third-party cookie feature, which makes me crazy. I think that's a very important thing. They've got that - we talked about that green address bar. That's, of course, an important part now of Firefox.

Steve: Yes, I'm very glad, the Extended Validation Certificate indication, yeah.

Leo: Well, what do you want to talk about today? What is on our agenda today?

Steve: Well, I've got a bunch of random errata. I'm not sure what we would call today. This has ended up expanding. I did say last week that I wanted to talk about the so-called Phorm Webwise technology. But I think we need to do this in two parts because I completely understand what the Phorm Webwise technology is, and it is really horrible. It's something which the three largest ISPs in the U.K. have announced they're going to support. A number of U.S. ISPs are at some stages of adoption. And basically it's a next generation of behavioral profiling, is the way they're calling it, behavioral tracking where these companies are installing equipment in and-user ISPs for the purpose of literally tracking what we do. And paying, essentially paying ISPs for the privilege of spying on us.

But I wanted to talk - I have a bunch of errata, and it turns out that because Phorm is not the only company doing it, I wanted to sort of give us an overview of this whole - sort of explain the way things have been done before, how this is different, what many of these companies are talking about today. And then in two weeks I want to expressly go after an explanation of how the Phorm system works because what they've done is extensive and amazingly intrusive.

Leo: Yeah. Wow. So any errata? Did we make any mistakes last week? Anything that...

Steve: Well, not errata. But I wanted to acknowledge the death, unfortunately, of two people. Of course you know I'm sure that we lost Tim Russert on Friday. He was in the studios of NBC at 2:00 in the afternoon, getting prepared for his weekly "Meet the Press" show. He had been vacationing with his wife and son in Italy. And he flew back early because he needed to do the prep for the show. He was 58 years old, and he saw his son graduate about a month ago. And I've been watching Tim every Sunday for an hour for at least the last decade. And it's just really sad that he died. It was a coronary thrombosis. A chunk of plaque that was in his veins came loose and took him out.

And then just, I guess it was late last night, we lost a famous Hollywood visual effects artist. Stan Winston died. Stan gave us the dinosaurs from Jurassic Park. He created Predators, Terminators, Aliens. He did the cool suits on Iron Man. And he died at age 52 of cancer. He had multiple myeloma. So he's no longer with us. So I remember seeing the credits of Iron Man scroll up the screen, and there was Stan's name, as it has been so many times for movies that I love. So I just wanted to acknowledge and mention, if anyone didn't know, that we lost those two people, that they're no longer with us.

Leo: Yeah, very sad. And it's...

Steve: Also - go ahead.

Leo: Oh, I was just going to say, it's a little scary for those of us like you and me in our 50s to hear about Tim's sudden demise. And I know you're a great fitness buff. We don't have to - anybody seeing you on camera knows we don't have to worry about you. You're in great shape. But I'm going to have to start thinking about my diet and exercise plan, too.

Steve: Well, it takes time. I give it - actually I was on my stair climber when I got the news last Friday about Tim Russert on MSNBC. I was preparing to watch Chris Matthews on his "Hardball" show, as I do. And it's like, well, okay, yeah, glad I'm working out while this is going on.

I've also recommended the encryption program AxCrypt many times, so I wanted to advise our listeners, those of our listeners who are using it, that there is an important update. As I understand it, it only affects Vista. Vista and AxCrypt don't get along due to Vista's address space layout randomization. We've talked about ASLR, which is one of the anti-hacking technologies that Vista incorporates where it randomizes the address space of applications to make it harder for malware to jump directly into known locations in the OS. And something about versions of AxCrypt prior to v1.6.4.4, which is now the current one, they might have had problems, apparently did in some cases, under Vista. That's been fixed. So there is an update to AxCrypt, which is a very nice standalone file encrypter. If you don't want to encrypt your whole drive, you don't want to, like, do heavy-duty encryption or have it present all the time, this allows you to perform state-of-the-art, good, strong, AES encryption very easily.

I wanted to come back to our mention last week of the Windows Bluetooth vulnerability.

I didn't know - no one knew anything about it at the time. I wanted to reaffirm that it's as serious as I was worried it might be. It turns out that anyone who has not updated their Bluetooth stack, who has got Bluetooth activated and have left Bluetooth discoverable, could be remotely hacked by somebody who sent a lot of service discovery protocol packets. There was a problem in the SVP protocol that allows, essentially, a remote code execution vulnerability. So any time there is a situation where radio is involved, of course, security is a little more troublesome. And that's definitely the case here. So you want to make sure that you've got Windows Update applied from our second Tuesday of the week [sic] update, which was last Tuesday.

Leo: So that was part of the update. So if you did apply that update, you're okay on the stack. And it's not on your phone, it's on your Windows machine that it needs to be updated.

Steve: Well, it would be anything that - I don't know about the portable edition of Windows, whether that was there. So it may very well be that the stack in Windows CE that many people have in their PDAs, it could have been affected, too. But certainly laptop-based systems. We know that that was an issue. Another thing that happened this week is that McAfee released a very interesting report. They did a first report about a year ago. And this is - they called it "Mapping the MalWeb." And so this next report is revisiting that. And it contained a whole bunch of interesting statistics. Anyone who wants to see this report for themselves, if you go to www - in this case you do need the www - .mcafee.com/advice. Again, that's www.mcafee.com/advice. I tried it without the www, and it's strange. It takes you to a McAfee page, but it says, oh, we don't know about advice on this machine. So you've got to do the www.

When you do, up near the top they talk about this "Mapping the MalWeb" report, which is a PDF, a 14-page PDF. But it had some interesting statistics that I thought our listeners would find interesting. Perhaps not surprising, of all of the top-level domains they tested, the Hong Kong domain, which is .hk, is the most risky top-level domain. Of the sites they tested, randomly looking at sites in the Hong Kong domain, 19.2 percent of these were infected with some kind of malware, meaning that there was some opportunity for anyone surfing to any, you know, a 19.2 percent chance that if you surfed to an arbitrary site in the .hk top-level domain, some sort of exploit was attempted against your web browser. The China domain, .cn, is number two most malicious top-level domain, with 11.8 percent of its sites trying to do some sort of exploit against your browser. And the most risky top-level domain is, that is, just overall, is .info, with 11.8 sites infected, which is up from 7.5 the prior year. However, overall, it turns out that overall very few sites worldwide are infected. It turns out that it's 0.0717 percent, meaning that overall, if you went to 10,000 randomly chosen sites, only seven sites out of 10,000 have any exploit code.

So we've talked a lot about the danger of surfing with your web browser to sites which are trying to exploit your browser. So I like the idea of having, from McAfee, some hard numbers about, okay, well, really, on arbitrarily chosen sites, what's the likelihood? On the other hand, there are clearly areas of the 'Net that are more dangerous than others, and sites like classes of sites which are more dangerous. For example, of all the sites which are download sites, and we've talked about the danger of acquiring malware or exploits against your machine in download sites, it turns out that 4.7 percent of sites offering downloads do have malicious content on them. So the download sites tend to be more dangerous by a, well, "tend to be," I mean, by a huge margin over non-download sites, just other types of regular sites.

Leo: So, well, I guess that's not much of a surprise, nor is it a surprise that Hong Kong and China are the difficult places. But it's good - do you think that, I mean, these guys have somewhat of an ax to grind; right? I mean, they're trying to prove that there's danger out there. I mean, I always get a little suspicious when I read about issues from people who make money on security, so...

Steve: Who profit from there being problems.

Leo: Right.

Steve: Right.

Leo: Just thought I'd throw that in. You have nothing to say about that, huh? You don't want to defend them, huh? No, but a lot of times I think, sometimes, anyway, that they may phrase the stuff in a scarier way just because, well, I mean, this is ultimately the reason they do these studies is to get you to buy their services.

Steve: True. Although it's a large and big and varied market now. And it's certainly no surprise to anyone that the world's got malware and browser exploits and spyware and all this kind of nonsense. So...

Leo: The thing that always amazes me is how much more widespread it is than one thinks.

Steve: Yes, yes.

Leo: There's just a lot of it.

Steve: Okay. So behavior targeting is the next thing that is really preparing to happen. And it's troublesome because it's something we haven't seen before. It's a new approach and a new technology that has not been used before. And it's causing a huge amount of concern among privacy advocates and among end-users. I mean, for a number of reasons. Some surreptitious tests have been done by ISPs, specifically BT in the U.K., where in 2006 and 2007, without telling their users, equipment was installed by the ISP into their facility which - by a third party, and a third party of some questionable reputation, specifically for the purpose of intercepting the web traffic of these users, and [indiscernible] things with it. So the issue is this is a very different style of profiling than what we've seen before. We've talked briefly about the problem with third-party cookies, that is, the idea that you have images, for example, on a website that are being served by third-party servers. And by default all browsers except one, Leo, I don't know if you're aware that Safari is the only browser that has third-party cookies disabled by default.

Leo: I think we discovered that. I think we were talking about that issue, and I went through all the browsers on my desktop, and that was the one that was off by default. Which is the right - and you say that's the way it should be.

Steve: Well, I believe the way it should be because it was never the intention of the guys at Netscape that created this cookie protocol - that basically added cookie technology, stateful user management to the web browsing technology - it was never their intention that third-party sites should be able to do this. But the clever people who wanted to advertising-enable the web said hey, wait a minute, not only can we be third-party servers of advertising on sites that people go to, but by having us, we as third parties put a cookie on the user's machine, then we'll be able to see where they go over time. We'll be able to, essentially, we as a third party build a persistent relationship with this, well, with everyone who surfs sites to whom we are providing ads. And their theory is that by looking at the sites that people go to, they can build up a profile of these people over time. And it ends up being more complex than that and actually of somewhat more concern because there are various ways that personal and personally identifiable data can leak out of a user's web browsing experience to essentially create more than an anonymous file of these people on the web. And this is fundamentally enabled by third-party cookies. So...

Leo: So the risk is that they could use third-party cookies to accumulate a profile on you by essentially following you around to sites that this third party, whether it's DoubleClick or some other ad agency, is serving.

Steve: Well, it's more than a risk. It is a feature of their business model. They brag about the fact that they are building profiles. They say, oh, because of the technology we have, the fancy stuff we're doing, our ads are going to be more tightly targeted to users, the idea being - and they say, oh, that's good for users because they're going to see ads more relevant to who they are. As if - I mean, all of their claims are legion in the industry. They'll say, for example, if we have figured out that you're newlyweds with babies because of the types of sites you visit, then we'll be able to serve you ads that are more relevant to your lifestyle or where you are in life. And again, so somebody who's in their geriatric years, they will have figured out that that's who they are. And so they'll serve ads from this big bin of ads, apparently, that they have, that are unique to the specific users of a generic website. So the point being that not everyone who goes to the site receives the same kind of ads.

Well, I mean, even that has concerned people. And there are many people who are security conscious and privacy conscious who have taken the time to disable third-party cookie tracking, that is, the idea being that you need a first-party cookie relationship with a site, for example eBay or Yahoo! or even, well, certainly banking sites are - more and more sites are requiring first-party cookies, typically anywhere that you logon. There is a cookie exchange with your browser so that as you move through that site's pages you're known by the site. And it's increasingly expected that the first-party cookies will be present. But arguably there is no defensible reason for using third-party cookies. Okay. So...

Leo: Except to make money collecting information about what you do.

Steve: Exactly.

Leo: Which is a very good reason for DoubleClick and Google.

Steve: And I want to say here, I want to make sure people understand that I'm not saying that this stuff necessarily needs to be turned off. I'm concerned that all of these companies say, oh, well, anyone who is uncomfortable with this can opt out of this technology. The problem is, I mean, it was like - it's the classic example of adware purveyors who say oh, no, we always provide opt-out provisions. It's like, well, if so, it's buried down in the fine print. And more often than not, when you tell people this is going on, they're upset, meaning they didn't know. And so I have no problem if people wanted to turn third-party cookies on. I'm annoyed that they're on by default on all browsers but Safari, and it's necessary to turn them off.

Leo: There's also an irony because people who run spyware programs that kill tracking cookies, when you opt out, at least with DoubleClick, it sends a tracking cookie to say don't collect these cookies. And if you used an ad block program or an antispyware program, often it kills the opt-out cookie, and you're back on cookies. They're on again.

Steve: Exactly. Exactly. Okay. So what Google has done with Google ads is, when a website says, okay, they set up a relationship with Google, and they say we want relevant ads to our site, what Google does is Google's technology looks at the page where the ads are going to be served, performs a keyword analysis, figures out what the page is about, and then Google's success is that from their pool of advertisers they use their own logic to populate the ads on the page so they're relevant. And I know that Mark Thompson has been messing around with this a little bit, curious to see, like, what level of relevance would Google's ads provide. And I think, you know, many people are [indiscernible] Google ads on an increasing number of web pages now. And Google does a pretty good job.

Now, the vendors of the behavioral tracking technology say, okay, problem with that is that there are sites that don't have pages where there's, like, available ads that are relevant to their content. Or you might have, like, a blogging site where there just isn't any clear topic for the page. There isn't anything that anyone, that an advertiser could lock onto to say that's what this page is about. So what the behavioral tracking people are trying to do is instead of putting ads on a page based on the page's content, they're purporting to put ads on a page based on the people, the behavioral profile that they've developed of the people who are going to be visiting the site. So there are a number of companies that are entering this game. This is just brand new. This is just beginning to happen. The company I talked about before, Phorm. There's a company called NebuAd, one called Front Porch, one called Adzilla, and...

Leo: Because we're running out of names, and frankly all of these names are terrible.

Steve: Oh, NebuAd.

Leo: Nebu.

Steve: Yeah, nebulous ads or something. Okay. And there's something called Adzilla and something called Project Rialto. So NebuAd, for example, they say to site publishers, and this is jargon taken from their promotional material, they say "NebuAd observes aggregated consumer activity across any site on the Internet without collecting and using any personally identifiable information about the consumer. NebuAd combines this [indiscernible] wide view of pages navigated, searches performed...." So they're seeing what searches you do. They're watching, essentially they're in your click stream. All of these companies, every one of them is installing equipment in the ISP's facility.

Leo: That's the important thing is that the ISP knows everything you do. And they're willing to give this information up. So do advertisers.

Steve: Right. Well, okay, for example, NebuAd says to ISPs: "To date the role of service providers has been limited to enabling but not participating in the online advertising revenue ecosystem. Whether you are a wired line or a wireless ISP with national or regional coverage, NebuAd offers a risk-free way to achieve stronger revenue growth and improve your average revenue per subscriber.

Leo: You know, we talked a little bit about this I think on a TWiT episode because Charter Communications, a big cable company and Internet Service Provider, announced this as - they spun it as, frankly, a valuable thing to consumers. If you read the FAQ at Charter's site, it says no, no, you're going to get ads that are more targeted to your interests. And it's not that they're replacing ads that are coming in, but they're willing to sell information about you to third parties so that the ads can be more targeted.

Steve: Exactly. Well, essentially the equipment is installed by these companies and at no cost to the ISP except for it's in the ISP's facility, so they have to make rack space and space available.

Leo: And maybe the cost of their reputation, but that's another matter.

Steve: Well, yes. That can be huge. There's been such a bunch of flak that's been raised by the Phorm system and the early technology two years ago that they were testing with BT. I mean, it was causing all kinds of problems. That early technology was inserting JavaScript into every page your web browser downloaded.

Leo: I don't like that.

Steve: So it was inserting their own code into the page for the purpose of setting browser cookies on the client, client-side browser cookies. Sometimes, because this stuff was so ineptly done, people doing forum posts using browser-based forums would get this code stuck into their forum post. Browsers were locking up. IE would lock up, and you'd have to use Task Manager to shut down IE because its use of the system would go to 100 percent, and IE stopped obeying its UI completely. All of this was brought to you at no charge by your ISP.

Leo: See, it's interesting because I probably blamed IE when that happened. I thought, oh, there it goes again.

Steve: Well, as far as I know this hasn't come yet to the U.S. It hasn't been done to us. Although the Phorm guys are actively soliciting U.S. ISPs. Adzilla, the Adzilla folks say to ISPs, "Adzilla works hand-in-hand with the world's leading Internet Service Providers to help them monetize their traffic, anonymize their data, and offer a better browsing experience to their subscribers." Then they pose the rhetorical question, "How does Adzilla work? ISPs install our innovative ZillaCaster device" - oh, goodness - "within their network environment free of charge." This won't cost the ISP anything. In fact, no, it's going to make you money. "ZillaCaster then enables the analysis of terabytes of real-time anonymized data flowing over the ISP's network." Yeah, over the ISP's network, which is to say all of the traffic that all of the ISP's customers are transacting. They're analyzing these terabytes of data in real-time and "leverage this data to offer precision ad preferencing information to publishers and advertisers." It says, "How does Adzilla help ISP monetize data traffic? When an advertiser pays for a targeted ad placed on Adzilla's advertising network, Adzilla shares the revenue with ISP partners."

Leo: Yeah. This is why they do it. They make - it's a moneymaker.

Steve: Exactly. "By using Adzilla's technology, ISPs create new online advertising opportunities, provide publishers and ad networks with audiences that deliver optimal results, and maintain optimal standards of consumer privacy."

Leo: I love this spin. By the way, I just checked, Charter is using NebuAd.

Steve: Oh, goodness.

Leo: So they're - I don't know if they're the first ISP in the U.S., sounds like they are, to do this. But boy, I think we should keep an eye on our Internet Service Providers. This is terrible.

Steve: Well, I'll tell you about NebuAd in a second. I have researched their technology. The good news is it's less bad than Phorm's, but it is also non-blockable. Whereas Phorm technology can be blocked. It's so bad. And that's what we're going to talk about in two weeks. And so just to finish up, to give people a sense for...

[Talking simultaneously]

Steve: Yes, Adzilla says in their promotional material, "Why is Adzilla's targeting so precise? Adzilla's ZillaCaster device, which sits within an ISP network environment, continuously analyzes the content of actual sites visited, ads clicked on, and keywords searched for each anonymous entity at any given moment to provide precision ad-preferencing information. Since Adzilla technology offers the most precise ad targeting in industry, publishers that participate in Adzilla-affiliated ad networks can offer premium quality inventory to advertisers at the highest possible rates." So, I mean, it's what we've seen before in the adware business. And it's that kind of, well, it's unfortunately the technology that end-users are not being informed of before it's brought to them.

Now, NebuAd, which is using a substantially less invasive technology than Phorm, they are basing their technology on hashing the IP and some other browser headers in order to determine whether the IP changes. NebuAd recognizes that over the long term end-user IPs change. So they're attempting to detect when the end-user's IP has changed. What they say they do, first of all, so this is essentially a filter technology, it's a shim stuck in the ISP's facility that looks at, essentially, all the queries being made by the ISP's customers. Oh, and it's important to note that this is only non-encrypted communications. They have no ability to penetrate, thank goodness, HTTPS SSL connections. So it's only non-encrypted pages that they're able to see. And it's also only HTTP traffic presumably to port 80.

But they are looking, they have access to everything that the ISP's customer does. So every page that you pull up, when you're browser-displaying the page, they have read the page and performed keyword matching, looking for important keywords that they use to tell them what this page is about. So they know that it's you by your IP. They are reportedly not putting any cookies or anything else on your system, which makes them vastly cleaner than the Phorm system we'll talk about in two weeks, whose cookie planting is beyond extreme. So they're just tracking you based on IP, which makes them cleaner. They say that if you are going to a health or, for example, a sex-related site, that they will not perform any filtering and tracking of that. What they do is they then broadly categorize the page that you're looking at into so-called "interest categories." And they have somewhere on the order of a thousand or more interest categories. And so they reportedly associate your IP with which interest categories you're searching to.

And then if you go to a site which is part of the NebuAd network, as these companies all call this, meaning that a website is getting ads served by NebuAd, then they will, because your browser is, for example, at CNN.com, but it's pulling images from NebuAd's servers, they'll see the IP which is requesting the ad, check their system to see whether they know anything about you by your IP and, if so, serve an ad which falls within this broad interest category delineation. So basically that's the concept in a nutshell, the idea being that they're not using third-party cookies in order to build a long-term profile of...

Leo: They don't need to. They've got even more information.

Steve: Well, and one concern is the household that uses a single IP and many machines because they're not disambiguating based on browser, exactly, because all the browsers behind a NAT router are going to use the same public IP. So that there is, unfortunately, some potential for cross-user leakage. That is to say, you know, Dad's using the computer doing whatever he's doing, and then...

Leo: But all that would happen is you would see Dad's ads if, I mean, right, that's all it means, it's just you're going to get ads that are targeted at Dad instead of you.

Steve: Exactly. Well, and the other thing, too...

Leo: It's not the end of the world.

Steve: With all of this, no one has even proven that this concept works, that they're actually, I mean, with all they're going through, I mean, all these companies are just in startup mode. They're like in the early beta-testing mode. In fact, over in Adzilla's site most of their site is soliciting - there are job postings for senior server engineers and people that are going to help them develop this Adzilla and their ZillaCaster technology. But even so, again, nothing has shown that this actually generates higher click-through rates and higher quality results.

Leo: It's a funny thing because advertisers have known for a long time that ads are less intrusive, less annoying, less resented by consumers if they're targeted. If the consumer is interested in buying a car, they actually enjoy new car ads. They look at them. So, you know, it's an invasion of privacy, but its net result is to give you ads that are less offensive to you and advertisers like better because they're not wasting money on advertising to people who aren't buying a new car. But it's the privacy implications that we're talking about.

Steve: Yes. And again, Leo, I don't have, I mean, given a choice - and unfortunately a large number of users apparently feel this way. Given a choice to have that or not, most users say no, I would rather not have any kind of profiles of any sort being made of my use of the Internet. And notice also that the ISP is generating cash for themselves, essentially by allowing their users to be spied on by third parties.

Leo: That's what bugs me.

Steve: Yes. And for example, I would not have a problem if, for example, your ISP said, if you would like to - if you are willing to have your use of the Internet profiled, we will give you a discount on your monthly service.

Leo: I'd like that.

Steve: Yes. And no doubt there would be a lot of people who'd say sign me up. I'm not concerned about being anonymously profiled. If the ads are more relevant to me, I want them, and I'd like to save $2.50 a month.

Leo: Right. It's a variation - I'm glad you brought this up. I tried to actually bring it up on a TWiT episode a couple of weeks ago, and people were kind of ho-hum about it. And I think it's because people didn't really understand what we were talking about. And more and more U.S. ISPs are looking at these technologies.

Steve: Well, yes. And so I'm glad it's getting attention. In two weeks - we're going to do our Q&A episode next week. In two weeks I want to take our listeners - this'll be a propellerhead episode, so I want to warn people in advance to get ready in two weeks to understand what this Phorm technology is. It has evolved in two years to - because what they tried to do two years ago where they were injecting JavaScript into people's pages, it just - it was a disaster. It backfired on them. I don't know if it's just that they didn't do it right or what the story was. These people, though, are not good people. They used to be called 121Media.

Leo: Oh, I remember them.

Steve: Yes, Leo. Yes, Leo.

Leo: Did they do, what is it, CoolWebSearch? What was it that they did?

Steve: They did something called "PeopleOnPages" and also did something called "Apropos." Apropos was one of the worst adware that used rootkit technology. It installed itself into randomly named directories. And then it installed a kernel-level driver to hook the API Windows to - and it used, it was a kernel rootkit that was in there hiding, inventorying people's machines and monitoring everything that they did. These are the people that bring us now this Phorm system. And in two weeks I'm going to talk about the technology that these guys have come up with. It's just unbelievably invasive.

Leo: KJ's asking in the chatroom if any mobile carriers are using this. Because then they really, I mean, they have your phone number, they really would know everything about you, wouldn't they. I mean...

Steve: Somewhere I saw, oh, it was - there's one of these companies called Front Porch that is - in advertising to ISPs says, "Monetize your network through advertising. Just make a new revenue stream through advertising." And get this. I love this. "Advertise at all stages of the user session, not just first login. Choose from a variety of high-value ad formats including Ultramercial," whatever that is.

Leo: It doesn't sound good.

Steve: It doesn't sound good. "Target users based on location or user preferences. Advertise to the right user anywhere they surf the 'Net." Oh. I mean, it's just in-your-face stuff. And then it says, "Among the popular uses, redirect subscribers' homepage requests to your portal. Redirect search requests to a partner web..."

Leo: That's spyware. That's spyware. That's adware.

Steve: Yes. "Create a walled garden of allowed sites for specific subscribers." So they basically, again, the ISP can do this because they have total control over your outgoing requests and your incoming data. So what we're potentially seeing now is this evolution from ISPs to passive bandwidth providers to saying, wait a minute, we want - here are these companies saying, oh, don't worry, we're going to take care of everyone's privacy. Everyone will be anonymous. If you'll just let us install our equipment in your facility and stick us in between you and your subscribers, we're going to pay you.

Leo: So, I mean, I guess you're saying that they should be more like a utility. Just sit back, give us the bits, don't get in the way, don't get involved.

Steve: Well, okay, yes. Again, my opinion is that users need to be informed, that if an ISP is going to be making money by monitoring what their customers do and by in any way providing that information to a third party as a source of revenue, whether the ISP justifies it saying that it's good for their end-users because it provides more relevant ads, first of all, it should not be opt-out. That never works. It needs to be opt-in. And if the ISP is concerned that not enough people will opt in - oh, yeah, gee, I wonder why - then they could do some revenue sharing and say, look, we're both going to make money if you allow the places you go on the Internet to be anonymously monitored and to have the pages you see change based on what this third party determines about you, we'll...

Leo: Well, there's intrusive and there's intrusive. I mean, if it's like Google ads, where - I guess this is what Charter is saying is what we'll do is we'll sell this information to advertisers, like maybe Google ads, Yahoo!, and so that they can be more tailored to you, even more so than they already are. That's one thing. If they're changing my home page and my search page...

Steve: Well, that's not - yeah, that's not how NebuAd works. NebuAd is a - wants to be an advertising network, much like DoubleClick, so that advertisers will advertise with NebuAd, and then NebuAd will get placements on high-profile web pages that users go to. And the idea being that supposedly there will be a higher click-through rate with NebuAd's better targeting, that the targeting is better because they're literally, based on the IP in the case of NebuAd, based on the IP of your connection, they're building a profile of the ISP's user. And, when they see that IP pull an ad from a different page, they choose which ad among their multiple ads they're going to serve the page.

Leo: Right. And I don't like that. But again, I think your point is perfectly taken. If they're going to do it, fine, they just need to say. The problem - and, you know, let us know, make us...

Steve: And they cannot be opt-out. It has to be opt-in.

Leo: Ah, good point. Charter's doing an opt-out thing. In fact, Ed Markey, who is a member of Congress, said that's not enough. Yeah, he said exactly that, I want it to be you choose to be a part of this. The real problem is, of course, there's not much competition among Internet Service Providers. It's not, you know, most markets have one, maybe two. And so it's not - if they both do it, it's not like you have somewhere you can go.

Steve: Yeah. I think, again, obviously the listeners to this podcast are going to be aware of this. In two weeks we'll be talking about the things that can be done proactively to block this kind of technology. There are some things that can be done in the NebuAd case. So but I'm not concerned about our listeners. Our listeners are already hip to all of this stuff. I'm pissed off that this is something that most people won't know about. And again it's just - I remember back when I was fighting with Aureate, that renamed themselves Radiate in the same way that 121Media has renamed themselves Phorm, because they ruined that name so they're now changing to a different name, people were furious to find out that this stuff was on their machine. And the Aureate people said, oh, no, all of our partners, our contract says they're going to make sure that users are advised. And I said, well, apparently users weren't advised, otherwise they wouldn't be pissed off like this. I mean, right?

Leo: Right.

Steve: People [indiscernible] I know about that. No, I mean, people were just going ballistic over the idea that this stuff was installed on their machine. So it's like...

Leo: I'm really glad you brought this up. I think it's such an important topic. And it is a little complicated.

Steve: It is a little complicated. Believe me, though. This is nothing compared to what we're going to do in two weeks. You won't believe what the Phorm people have done.

Leo: Oh, boy. All right.

Steve: Oh, yeah.

Leo: So let's...

Steve: You know, I never shared one of my SpinRite...

Leo: I was going to ask you about that, do you have a SpinRite letter? Usually you...

Steve: Right. Normally I do it at the front, I just forgot. I did have it written down here in my notes. I just had a really neat note that I got from a dad. The subject of his note was "One Happy College Student." And this is William Turner, who said, "I can't [indiscernible] where to send this." I think he must have sent it to our sales address. So he says, "I hope this forum is okay." Or maybe he posted it. I can't really tell where it came - oh, no, it came through sales. And he says, "I wrote this about a month ago, and I'm finally getting around to mailing it. And he said, "Dear Steve, I'm a long-time listener to Security Now!. I bought SpinRite about a year ago and have used it for maintenance purposes ever since. A few days ago I got a call from my daughter, who was out of state attending college. She was crying like the little schoolgirl I remember. She then explained the Blue Screen of Death that all those who use a computer fear. I told her not to worry, it could be fixed. Then the tears really began to flow. She said that a semester-long project was on the drive with no backup of any kind. 'Daddy, what can I do?' She said, 'I need you to come here now.'

"Well, she's about 2,200 miles from home, so that was not an option. I told her about SpinRite. I quickly determined that I would FedEx my copy of SpinRite to her today. When our phone conversation ended she was sure a failing grade was the only option in her future. This morning, however, I received a call from guess who, my little girl, who thinks I am the smartest dad ever. This conversation was filled with jubilation and amazement. She said, 'It fixed my hard drive. My laptop is working, and I just backed up all my documents.' Her worries of a few days ago were all but forgotten.

"Steve, thanks for helping me appear like the dad who knows it all. You saved my daughter many sleepless nights. SpinRite is a must for everyone who owns a computer. All parents should not send a son or daughter away to school without a copy of SpinRite. Thanks for your great product and all the hard work you do." Signed, William Turner. And he may be listening to this right now. So thank you, William, for sharing that story. That's great.

Leo: Really, that's the kind of thing, everybody should go to school with a SpinRite disk, absolutely. We like that idea. So, Steve, we're going to - next week is going to be Q&A week. So we'll talk about Nebu - or no, is it NebuAds or Phorms that you're going to talk about?

Steve: Going to talk about Phorm in two weeks, about what they - the hoops that they jump through and what they do to users in the process in order to achieve this, ugh, this questionable, basically spying on and profiling, courtesy of users' ISPs.

Leo: How do people ask questions for next week's episode?

Steve: As always, go to GRC.com/feedback.

Leo: Okay. That's simple. There's a form right there for you, GRC.com/feedback. While you're there don't forget to check out all the other great things GRC has to offer - SpinRite of course, but also ShieldsUP!, which is free, to check your router. There's lots of software: Wizmo, all sorts of free security tools, utilities and more at GRC.com. And show notes for this show, 16KB versions for the bandwidth-impaired, and Elaine's great transcriptions so you can follow along. You can read along as you're doing this. That's GRC.com.

Steve: Leo, while you were talking I was reading the chat log going by. And there's been some question actually going back and forth about whether SpinRite works on iPods. So I thought I would answer that directly and remind people, maybe these users don't remember, but there was one testimonial that I read where someone did use SpinRite and took the drive out of his iPod and hooked it up to his PC. And then when it fixed his, remember he had like a collection? It became a joke. Everyone was giving him their dead iPods. And he had, I don't know, like 20 or 30 of them lying around as doorstops, bookends and things. And so he fixed them all and then gave them all back to them with all their music intact.

Leo: That's the amazing thing. That was an amazing story, yeah. So I guess we're out of time. But we will be back next week with more of your questions and more of Steve's answers. And then the following week we'll continue this conversation, talking about these, well, I guess programs or boxes that Internet Service Providers are using now to spy on you, ostensibly to provide you with better ads but really to make some money.

Steve: So I just can't wait to tell our listeners about the technology that has been employed. It's just mind-bogglingly bizarre. And frightening, arguably. It's a mess.

Leo: It's terrible By the way, Steve, while we've been talking - as I mentioned, we record this on Tuesday, which is the download Firefox day. And even though Firefox's site has been really hammered - and Sargit in our chatroom is pointing out that it looks like the hammering is coming from an applications server that can't keep up because he can ping the site, but the application server is just not serving the pages up. I guess they didn't expect this, even though they said they wanted to set a Guinness world record for the number of downloads. Over 200,000 downloads just as we've been talking, Steve. They're up to three quarters of a million. And they're doing 11,000 downloads a minute now. So it's pretty impressive. They're really...

Steve: Well, I've got to say I've been doing, for the last several months, Leo, I've been working intensely on the issue of cookie handling. Most of the major browsers out there have cookie-handling bugs which apparently have gone unknown for a long time. IE does. Firefox 2 does. Opera, I think Opera is among the best. And Firefox 3 has got it nailed now, too.

Leo: I'm very glad to hear that.

Steve: So both Opera and Firefox 3 I'm very impressed with.

Leo: Everybody should download it. It's a great program. And everybody should listen to Security Now! every single week. We'll see you on Thursdays. And go to GRC.com for your copy. And if you want to go back through all 148 previous episodes, they're all there at GRC.com/securitynow. Thank you so much, Steve. We'll see you next week.