SECURITY NOW!

Transcript of Episode #206

Mega Security News Update

Description: A LOT of security news transpired during the three previous weeks since Steve and Leo last recorded live. So instead of the regularly scheduled Q&A episode (which is moved to next week), today they catch up with this week's "mega security news update."

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-206.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-206-lq.mp3

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

Leo Laporte: Bandwidth for Security Now! is provided by AOL Music and Spinner.com, where you can get free MP3s, exclusive interviews, and more.

This is Security Now! with Steve Gibson, Episode 206 for July 23, 2009: Security News Updates. This show is brought to you by listeners like you and your contributions. We couldn't do it without you. Thanks so much.

I've only been gone for two weeks, and I can't talk anymore. Hello, Steve Gibson. It's Security Now! time.

Steve Gibson: Yo, Leo. Actually it's been three weeks, hasn't it? Because I had a 21-day vacation. So I would think you did, too. Or I guess you got back before this.

Leo: I had to be here on Sunday and do the radio show and TWiT. But it's, you know, two and a half. I don't know what it is. But anyway, it's good to be back. Although maybe you can explain this to me. I'm going to have to find somebody, Kiki or Maxwell or you or somebody to explain this, why it is that jetlag is so bad when you're going west to east, and so mild when you're going east to west.

Steve: I do not know. Not having experienced much of it myself. When I was coming to you to do the shows in Toronto, I was back the same day or the next day.

Leo: Yeah, you didn't have time.

Steve: But you're right. My solution has always been just to sleep a lot. And when you finally wake up, you're like, oh, okay, I'm here now.

Leo: Sleeping doesn't help. You know, I couldn't get to sleep until 4:00 in the morning this morning. I'm just lying awake like this, [humming]. I mean, I'm in bed.

Steve: Maybe cabernet is my secret. Because I always mix in some - I mix in some cabernet, and that really seems to solve the whole jetlag problem.

Leo: [Singing] Cabernet is what I need. Dr. Mom says she's going to help me. She says, "Call me later, I'll help you."

Steve: Okay.

Leo: I've tried, like, the melatonin. You take the melatonin. I've tried...

Steve: Well, so you're still back in readjusting mode.

Leo: It took me two weeks last year when I came from Australia. This is roughly the same. It's...

Steve: Wow.

Leo: Yeah, it's - I'm expecting two weeks of kind of waking hell. And, you know, I do, you know, I stare into the sun, and I go outside and walk with the bright sun because you're supposed to tell your body - somebody told me if you take your shoes off, your feet somehow - that can't be right. I think I should go outside naked.

Steve: There was some movie where someone gave someone else advice, I think Richard Gere, for some reason I picture him.

Leo: Yeah.

Steve: Something about taking your shoes off and curling your toes on the carpet or something.

Leo: Yes, yes. That's what I've heard. But that makes absolutely no sense.

Steve: None at all, no.

Leo: That's like saying pinch your arm flab, and that will fix everything. That makes no sense. Steve, how are you? Has it been - now, for those who don't know, Steve is adamant about this, will not miss an episode. So we prerecorded the last - the last three episodes? Something like that.

Steve: Yeah, we double-recorded the two prior weeks before your departure so that we would have two extra ones to fill in while you were gone. And it worked. And here we are back. And we do have a bunch of catch-up to do because we haven't been live recording. In fact, this week is the "mega security news update" episode of Security Now! where we're going to talk about everything that's happened while you were off cruising around in Asia, and I had my two weeks off from recording. And then since this would normally be a Q&A, and we have also not done any Q&A for a long time live because we haven't been able to, the next two weeks are going to be Q&A episodes, which will finish off our fourth year.

Leo: Wow.

Steve: Of Security Now!.

Leo: Fourth? Wait a minute, no. Beginning our fourth. Finishing?

Steve: No, no, no. No, no, no.

Leo: We've done four years? I guess we have.

Steve: This is Episode 206. So we'll do 207 and 208 in the next two weeks.

Leo: That's four years.

Steve: And that's four times 52, which is 208. So, yeah, at the end of our fourth year, starting into year five.

Leo: [Laughing]

Steve: Yay.

Leo: Well, congratulations. And early happy anniversary. I did, I was, when I was in China I wasn't completely in touch with the news. But I was paying attention, looking for security updates and flaws. And it seems like there were a few things that happened.

Steve: Oh, there's lots of things going on.

Leo: While I was gone.

Steve: Before we get into that, I had a couple - I had just one little non-security note. I know this is of interest to you. It certainly was for me. The Economist is now available on the Kindle.

Leo: Yeah. I saw that before I left. I thought that's great news, yeah.

Steve: The Economist magazine. And Barnes & Noble had a big news announcement a couple days ago. They formally announced they're going to get into the eBook business and compete with Amazon and the Kindle. There's an interesting technology that was shown at a recent demo conference. The company is called Plastic Logic. And they've got a competing technology. I've not looked at what the technology is. I did check out the eInk technology that Amazon is using. But this literally, they've got a flexible plastic sheet which displays monochrome images. And they've got a reader. It also - it includes a touchscreen. So their UI is touch-based. They don't have physical controls. And apparently Barnes & Noble will be - I don't know if they're going to be OEMing it, or if they'll be tied into the Plastic Logic storefront. Because the Plastic Logic reader has - I guess the Plastic Logic folks are doing some sort of an eBook system themselves. So Barnes & Noble apparently will have some sort of arrangement with them.

But that was the announcement, was that Kindle will have potentially a major competitor that also has a brick-and-mortar interface to the public, not just an online, web-based interface. So, I mean, that could help a lot of people who want to go see one of these things rather than just ordering it blind and hoping they like it when it arrives.

Leo: Do you think it'll be better than the Kindle screen?

Steve: It looks pretty much the same to me.

Leo: Yeah.

Steve: Questions would be resolution. The guy who was demoing it...

Leo: Bur the DX, they say that the DX is better than the Kindle 2 in terms of screen contrast and clarity.

Steve: Well, you - I don't really see any difference. I have both. And in fact...

Leo: I'll tell you why I'm asking. I left my Kindle on the airplane.

Steve: Ohhh, Leo. Oooh, ouch.

Leo: So I - actually I looked at the DX.

Steve: Wait.

Leo: But I remember you didn't like...

Steve: This is not the first time you've done that. Or am I thinking of something else?

Leo: I left my Sony 505 on the...

Steve: That's right, the Sony, the 505.

Leo: Yeah. And so the next Sony I got, I got engraved with my name on it. But now I don't use that anymore. And the Kindle didn't have really any, you know, it has contact information inside it, but I don't think they looked. You know, I knew that I'd left it on the plane after I went through customs. And I went right to the desk, and they said, no, we don't have it. So somebody probably snagged it as they were walking out. They said, hey, some idiot in business class left his Kindle. He can afford another one.

Steve: Well, I have to say I'm beginning to see them, which is really interesting. There are at least three other Kindles that I've encountered, people reading them at Starbucks or in a restaurant or...

Leo: Yeah, I think they're much more common than I thought they'd be.

Steve: Yeah, I mean, I think it's really beginning to happen.

Leo: Well, they dropped the price to $299, so.

Steve: Yes. And frankly, well, this morning when I was out early getting some blood work done for my Vitamin D study that I'm going to be doing on myself, like does the sun really produce Vitamin D, I had my small one...

Leo: Steve, not content to accept years of science, is doing his own, walking around naked or something. I don't know what he's doing to test this.

Steve: Well, yes, actually I'm thinking probably that I will be getting full-body exposure in order - you know, brief - in order to...

Leo: What, are you going to become a nudist? What are you going to...

Steve: In order to generate, well, I have the ability, I have a location where I can't be seen. And I just sort of - I'm going to give it a try. But...

Leo: I might try that in my own backyard. For jetlag that might be the solution.

Steve: The reason is that apparently we should be getting much more Vitamin D than we do. We used to get it from the sun because just 30 minutes of sun exposure generates about 10,000 IU of Vitamin D. Yet supplements contain 400, which is what the RDA has set, or that is the RDA. And it's very difficult to get much in your diet. So now that we're wearing clothes and we're indoors, we're not getting the vitamin, we don't have the production of Vitamin D we should. And...

Leo: Of course in those days people didn't live long enough to have to worry about skin cancer, so...

Steve: Yeah, and frankly, Leo, I'm wondering how much that's overblown. I mean, there are apparently people who feel, and I haven't looked at this at all, that all of this slathered-on sun protection is really bad for you, too, but better than skin cancer. But you don't need a lot of sun in order to generate enough Vitamin D for the day, just 30 minutes. Which probably is, I mean, it's not like you're going to become crispy and be in the sun all day. But my point is that, once I start adding Vitamin D to my daily routine, which I haven't yet, I'll never want to stop it. So I only have one opportunity to sort of measure my Vitamin D level just the way I am now. And so that's what I did this morning.

My point was, though, before I got off on this tangent, was that I have both Kindles, the DX and my Kindle 2, and I took the Kindle 2 with me because it is so much more convenient as just a general-purpose reader. The DX has a magnificent screen. I loaded the - I had Amazon send a copy of the Economist to both so that I could look at them both sort of side by side. And the DX is beautiful, but you really do feel that it's too large, unless you want to be looking at PDF where, you know, it excels for that kind of performance.

Leo: That's what Dwight Silverman said, too, of the Chronicle. He said he couldn't lie with it in bed. And frankly, that's when I read most of the time is when I'm in bed. And he said it's just too big to hold up.

Steve: And I'll tell you, I really miss having navigation on both sides. I liked the extra...

Leo: Yeah, I'm a lefty. I need that left button.

Steve: Yes. As am I. And for the same reason. It's really nice. So were I you, I would replace it with a K2.

Leo: Good, because that's what I - I said, I'm not waiting till they find it, if they find it. I was in the middle of this great book I was telling you about...

Steve: And even if they do, you need a spare, clearly, so that you...

Leo: Oh, man. I'm in the middle of this Kim Stanley Robinson Mars book which is fantastic, "Red Mars." And I can't - and it was one of those I couldn't put it down the whole time I was in China.

Steve: And I've got mine loaded in the Kindle. Haven't started yet.

Leo: Oh, you're going to like it. It's really good hard science. And what's nice is, just like Peter F. Hamilton - by the way, we'll get to security in a moment - just like - we got a lot - we have to catch up. Just like Peter F. Hamilton, he's very good at characters. And yet the science is - you're going to love this because it's clear that Kim felt like he wanted to do the research so that it would be this is what we have to do if we're going to explore Mars. And as we get closer, I think get closer and closer to, you know, doing that, he has to solve all the issues. And you're going to love it. I mean, the science in it is fantastic. Lot of geology because Mars is a rock.

Steve: Yeah.

Leo: Fascinating. Oh, it's one of my - I'm really loving it. You're going to love it.

Steve: Oh, cool, cool, cool.

Leo: But I'm halfway through, and it's like, I need my Kindle fix. All right, Steve Gibson. Patch Tuesday was last week.

Steve: Yes, it was. And there was a bunch of stuff fixed. I wanted to start by giving our listeners a little bit of news about Yubico and the YubiKey.

Leo: Oh, I got, like, three YubiKeys in the mail the other day.

Steve: Okay, are they blue?

Leo: Yeah, they're the new ones.

Steve: Aha. That's the news, is that they only made 150. So what you have are very rare, limited edition, blue YubiKeys. They are the new dual function. Remember that the YubiKey can either function as a one-time password system or as a long, but fixed, password. The way they implemented the next version of the YubiKey, which Stina calls 2.0, is that you have both functions, or you have any two, either two different one-time passwords, two different fixed passwords, or one of each. And that you're able to trigger with a single contact. So there is a special offer, though, that they're making for our listeners. Reading from Stina's note, she said, "Also I wanted you to know that Yubico has offered existing customers a 40 percent discount when ordering up to nine units of 2.0 YubiKeys before the end of July. If you would like to, we would be happy to offer the same discount for Security Now! listeners, independent of whether they are Yubico customers or not."

Leo: Well, that's very nice.

Steve: "If you like this idea, please tell your listeners to enter the coupon code, SecurityNow, all one word" - and she has a capital N, I don't know if their coupon code is case-sensitive, but capital S-e-c-u-r-i-t-y capital N-o-w - "in the ordering process on Yubico's web store, and they will only pay $15 per key instead of $25. We would have the discount campaign for your listeners open for four weeks after your podcast, whenever in time this would be sent out." So I'm notifying all of our listeners that there's a special opportunity to purchase these new 2.0 version YubiKeys which are the dual function, for 40 percent off, $15 instead of $25, if they enter "securitynow" as their coupon code in the Yubico store. And that's Yubico.com. And I'm sure you could navigate to where to purchase them from there.

Leo: Cool.

Steve: So that's news from Stina Ehrensvrd at Yubico. So, yes. A bunch of, well, all, I mean, pretty much in the time since we last spoke, Leo, everything has been updated. Nothing is the same. Last Tuesday, July 14th, was the second Tuesday of the month. Which is interesting, I mean, it's the latest you could have a second Tuesday of the month because the first was on Wednesday two weeks before that. So the 14th is the farthest into the month you could have the second Tuesday. Three critical updates from Microsoft and three important ones. Microsoft has said that they expect exploits for all of the vulnerabilities that were addressed. There were problems in Windows; Microsoft Office; their IAS, which is Microsoft's Internet Acceleration Server; and even their Virtual PC and Virtual Server products.

In the case of Windows there was a very widely publicized, actually, Microsoft announced this beforehand because it was a zero-day exploit. There were exploits happening on the 'Net, so they'd let everyone know. They had the MSVidCtl ActiveX control had a buffer overflow which could allow arbitrary code to be executed just by visiting a website that would invoke that control using scripting. So that they fixed.

There were two patches in what they call the Embedded Open Type Font Engine, EOT. And that was exploitable from a website or email. Apparently websites and email are able to, like, specify that they want a specific web font embedded in the page, and that invokes this font engine on the fly, this open type font engine on the fly. And there was a problem with that, which Microsoft fixed.

And you may remember we talked several weeks ago about Publisher having a problem, that if you opened a Publisher file, if users opened a Publisher file that was part of, like for example attached to email, that could cause a problem. And that was one of the other things that they fixed. And then also there was a different problem with a video ActiveX control where Microsoft has told people just to set the kill bit. And I've got a further note about that a little bit later, so we'll come back to that because there's a Knowledge Base article that allows people to fix this. That's important because that was not included in this patch, and it is being actively exploited now.

Leo: So this is the one - this is one hole left open.

Steve: Yes. And this is a zero-day exploit, actively being exploited now. They apparently found out about it the day before the second Tuesday, not in time to fix it. I don't think they're going to do an out-of-cycle patch, but they've got one of those little fix-it buttons where you just - or the Fix me button where you can just click it. And basically all I does is it sets these so-called "kill bits" that prevent this control from being instantiated by Internet Explorer. And of course our listeners are hopefully just not using IE anymore. I mean, none of these are problems if you're not using Internet Explorer. If you switch to Firefox, which is what we recommend, you're not having this problem.

On the other hand, 3.5 of Firefox did have a critical memory corruption flaw in its Just-in-Time JavaScript compiler fixed recently. It's now at 3.5.1. So anyone using 3.5, and I know that you are, Leo, I'm holding back. I'm staying with Firefox 3 until 3.5 settles down a little bit more.

Leo: Oh. Yeah, I'm using it. I went to 3.5.1.

Steve: Yes. And so...

Leo: But that's not enough.

Steve: So, well, no, no. 3.5.1 is current. They fixed this Just-in-Time JavaScript compiler problem.

Leo: Oh, okay.

Steve: And apparently there were some performance problems, some startup problems with 3.5, like having a really slow startup in Windows. And so they say that they also addressed several stability issues and this performance problem that was causing a real slow startup in Windows. I know that my tech support guy, Greg, had upgraded himself to 3.5 and was really seeing Firefox being unwilling, I mean, just, like, really slow to start. And so he said, wait a minute, I thought it was supposed to be faster. And so apparently they fixed that in 3.5.1. I'm hoping.

Leo: That's a Windows issue, yeah, and it has to do with loading temporary folders for randomization.

Steve: Interesting.

Leo: For encryption, yeah.

Steve: Oh, okay. And over on Firefox 3, where I still am, that had an update also. It's now at 3.0.12, which is the current version. And in fact when I fired it up this morning I got the upgrade opportunity just now. So that's fresh off, you know, hot off the press. There were four things that were fixed there. There was a crash and remote code execution problem using scalable vector graphics. We don't hear about that that often. But scalable vector graphics is a technology that really, I don't know, for whatever reason it hasn't taken off that much in terms of actual deployment.

Leo: There's been Flash out there and...

Steve: Exactly, lots of competition from existing technologies which do the job.

Leo: Right.

Steve: There's also a heap integer overflow in this Firefox 3 in its font glyph rendering libraries that was fixed. There was a problem with Flash player unloading that was able to cause a remote code execution, of all things, when the Flash player was done. So the way it was able to unload, the bad guys were able to cause a problem. And they were also - there's some sort of a crash that had evidence of memory corruption, that just sort of referred to it generically. All of that's fixed in this 3.0.12 of Firefox. And you know me, I'm just - I'm going to wait a while before I go to 3.5. I ultimately will, but I'd like to let it settle down a little bit and get the debris shaken out. I know you, for the stuff you do...

Leo: It's a lot faster, you know, so.

Steve: It really is?

Leo: Yeah. That's the main reason.

Steve: I did update to it by mistake, and I found that none of my add-ons said that they were compatible. How are you seeing...

Leo: That must have been when it was still a beta, I'm thinking. Because once it came out in a release, all my add-ons worked. You know, sometimes it takes a while for the add-on guys to update.

Steve: Just to - right.

Leo: So maybe, you know, I'm not using NoScript, so it might be that one does not work. But all the ones I use...

Steve: I had all of mine, actually. So something must have been strange.

Leo: I don't know. I mean, we're not using the same ones. But that was true in the beta that a lot, almost all of them didn't work. And then once 3.5 came out officially, almost all of them did work.

Steve: And so AdBlock Plus, for example, do you use that?

Leo: No.

Steve: Okay. I think what I'll do is I'll do a test install and see whether the things that I care about are ready yet. But again, in general, I'm not in a hurry to jump on the latest bandwagon because those are just not secure.

Leo: Yeah, yeah. I don't know. I mean, you know, you get security updates forever anyway; right? It's not like...

Steve: Yeah, yeah. Well, but tried and true, I mean, you want to let it settle down. You'd like, for example, there not to be a really big problem that was not known. For example, have you heard about the iPhone SMS problem?

Leo: No, tell me about that.

Steve: Oh, we'll be talking about that in a minute. Anyway...

Leo: Oh, boy.

Steve: So, and that's not been fixed yet, and that'll be introduced at the Black Hat Conference this weekend.

Leo: Great.

Steve: But Google Chrome has also had an update. There was a problem in the Apple WebKit browser app framework, a heap-based buffer overflow vulnerability. And once again, it was just one of these random things. A specially crafted regular expression in JavaScript was able to cause a remote code execution, probably contained within the Google Chrome sandbox, that is, you know, Google is saying that. They're deliberately withholding further details until more users have updated. I did check, fired up one of my virtual machines that has Chrome in it. And sure enough, now I'm up to where everyone should be who's using Chrome, all 3 percent of you on the 'Net, and that's version 2.0.172.37.

Leo: But that happens kind of automatically, without your even knowing about it; right?

Steve: Yeah. So you're probably going to be current already. Although I did have to go to the About box, where I found Check for Updates, and then I was told that there was one. Although I didn't - I wasn't using it, and so maybe it was going to take a while and then do its check and verification. So then there was a different problem with it, where a malicious site could cause it to allocate huge amounts of memory and force a crash and, in the process of crashing, cause arbitrary code to run. So you would crash the browser, but in the process malicious code was able to get injected into it. And while Google was doing that, they also updated their V8 JavaScript engine to the latest version, which is 1.1.10.14. And then they also updated Gears to the latest version, which is 0.5.25.0. So that brings Chrome current.

And then Safari also had an update. We last left off with version 4.0.1 that we talked about a few weeks ago. Now we're at 4.0.2, which fixes two flaws. One's not so bad, a cross-site scripting flaw, but you'd like to not have any of those. We'll be talking about that later in this episode in another context, in the context of web-based appliances that have, like, real problems. But there was a memory corruption issue in Safari 4.0.1 and earlier that could be exploited to crash the browser or to execute arbitrary code, just by visiting a web page. So and that affects both Windows and Mac OS X versions of Safari. So you want to be sure that you're running 4.0.2.

Leo: Yeah, I noticed that update, and I didn't - they don't really tell you why.

Steve: Yeah, interestingly enough, Microsoft tends to be the most open of any...

Leo: Yeah, they really are, yeah.

Steve: ...of these companies because, you know, they've got to be. They've taken their lumps, and they were the pioneer with insecurity. So I think their policies are pretty well mature.

And lastly, I had a really nice SpinRite note from a guy who sounds like he's not easily impressed. And, I mean, this is one of those where, okay, I'm not making this up. This is Brad Schick, who wrote to tech support. I don't think he's a listener. But he just said, "I seldom send out praise for products because I expect to get what I paid for. So I generally consider praise unnecessary. In this case, I was so impressed with how well your SpinRite program worked that I must tell you it is truly remarkable. My computer had locked up while in screensaver mode. Nothing would bring it out of the lockup, so it had to be shut down via the power button. Upon restart, it would start to load XP for a count of 14 seconds. Then it would flash the Blue Screen of Death for one second, then go to the problem screen, asking if you want to start Windows normally, in safe mode, safe mode with networking, et cetera."

Leo: I hate that.

Steve: [Laughing]

Leo: Hate it when that happens.

Steve: "Trying to boot in safe mode or any of the other options proved to be futile since it would make the same loop again. XP attempted to start, Blue Screen of Death, then the safe mode option screen. I was skeptical that a program on a disk would be able to fix my problem. But after booting to SpinRite and having it do its magic for the Data Recovery Level 2 in only 17 minutes," and he says, "(17 minutes, it's not a typo)," he says, "it had finished its work and found and repaired a bad sector. My computer then booted normally and has been working perfectly ever since then. Your SpinRite program is easy to use, and it is truly amazing at how well it works. I will be spreading the word about SpinRite and the other programs you offer. Also, in regard to the price, it would have cost more to take my computer to a shop for repair, and that is not factoring in the time lost to do so. With SpinRite I have a tool that can be used over and over and over. SpinRite is an incredible product, just incredible. Regards, Brad Schick."

Leo: isn't that nice.

Steve: So thank you, Brad.

Leo: Don't you love getting email like that.

Steve: Oh, yeah, well, I mean, when we solve the problem. And he's, I mean, really addresses the benefits of SpinRite, what it does. And, I mean, even saying yes, it would have cost more. And besides, the shop would have just run SpinRite on it anyway.

Leo: Do you know for a fact that a lot of computer repair places use SpinRite?

Steve: Oh, absolutely. It's their secret weapon. They just say, oh, just run SpinRite. And then they don't spend any more time, and they charge hundreds of dollars. Thank you very much.

Leo: Yeah, I want to ask you, and I don't know if you've prepared anything about it, but you know Google announced an OS, I guess based on kind of Linux, but also with Chrome as the centerpiece of it. I'm kind of curious, especially with all these security flaws we've been talking about. And you're...

Steve: Chrome OS. I don't - I know of it. It generated...

Leo: Nobody knows anything about it because Google said nothing.

Steve: Right. It generated a tidal wave of news because it's like, well, because the way it was put out was this is going to compete with Windows. This was like Google's battle against Microsoft. And the other thing is, it's supposed to start up in two seconds. You turn it on, and it's, like, there. Basically it sounds like a very fast boot of Linux, running the Google browser basically, running Chrome. They're calling it the Chrome OS. And they're, of course, taking the web-based model where you would be connected. You'd have apps in cloud...

Leo: It's cloud computing, yeah.

Steve: Yes, cloud computing. Although apparently you are able to bring local copies onto your machine so that, if you don't have a live connection, you can still do things.

Leo: Right.

Steve: So it'll be calendaring and office app suite sort of things and the stuff that Google's doing now. They're just saying, okay, we're going to - you really don't need Windows. It won't be something you run - you won't run our browser on top of Windows. You'll run it on top of nothing. And presumably for free.

Leo: Yeah? As are all versions, or almost all versions of Linux.

Steve: Right.

Leo: Yeah, it's very interesting. But we'll find out more about it in a year.

Steve: When it happens, we'll definitely be bringing news. And no doubt updates to that, too, now.

Leo: Let's take a break. When we come back you have more security news? We should mention...

Steve: Oh, my goodness, news, news, news, news, news. We have an iPhone problem; a zero-day exploit in Microsoft; big news about Phorm, our nemesis in the U.K. McAfee had problems. Remember about - certainly you probably heard about the distributed denial of service that was launched against the U.S. and South Korea. I've got the whole tune-up on that. News about Pirate Bay, a survey about people and spam...

Leo: Boy, you go away for three weeks, the whole world goes to hell.

Steve: Some more Amazon news; cyber warfare may be becoming offensive; and a problem with embeddable web servers in devices. So lots of stuff to talk about.

Leo: All right. We'll get to that in a bit. I should mention that normally on a mod 2 episode like this we would be doing Q&A. But we're going to do two, you want to do two Q&A next week because we need to get caught up on the news.

Steve: No, no, I want to do a Q&A next week and the week after.

Leo: I mean two in the next two weeks, I mean, yes, yeah, yeah.

Steve: Yes, exactly.

Leo: So get your questions to Steve at GRC.com/feedback.

Steve: Yes, yes, yes.

Leo: And if you have a question, we'll get to those in the next two weeks. All right, now let's see what's going on in the world of security.

Steve: Okay.

Leo: We've got all - that was just patches, folks.

Steve: That was just patches. What we have now are things that are not yet patched. This coming weekend, starting on the 25th, is the - so the 25th through the 30th, I think, is the next annual Black Hat Conference in Las Vegas. Always interesting things are being shown. What is being shown this weekend is a remote execution vulnerability in the iPhone's SMS handling.

Leo: Which is - so you mean - well, I'll let you explain that. But it sounds like somebody could send me a text message and hack my phone?

Steve: Yes.

Leo: That's not good.

Steve: And there is no way to turn off text message reception on the iPhone.

Leo: That's right.

Steve: It is a zero-day exploit. It has been demonstrated by a security researcher. He has agreed with Apple that he will not release details until this weekend. So expect an iPhone patch. Apple is frantically working on fixing this.

Leo: Wow.

Steve: But this allows any iPhone to receive a text message and be taken over. Arbitrary code can be executed...

Leo: Somebody just sent me a text message that says "You've been hacked." [Laughter] They must be listening.

Steve: For example, they could determine where you are by polling the phone's GPS.

Leo: What?

Steve: They could turn on the microphone and listen to what was going on.

Leo: Oh, my god.

Steve: They could join the phone to a botnet, recruit it to participate in a botnet.

Leo: Because it's a computer.

Steve: Well, see, yes, that's exactly right. It is a full-power computer. And it is like the - and it's relatively new, and the software is still being polished.

Leo: Well, it's three years old. It's not that new.

Steve: Well, but they keep changing it. I mean, so there are...

Leo: Yeah, the version 3 is relatively new, yeah.

Steve: Exactly. And, I mean, change is - not only is complexity the enemy of security, but so is anything new. Which is why I'm not going to Firefox 3.5 yet. It's new. New is bad. I mean, it's just fundamentally bad.

Leo: Has he said if there's any way of knowing if this has happened?

Steve: No. Now, initially he was crashing the iPhone. When he gave a demo, the person who was the target looked up, and it just said "No Service," so the phone had crashed. But he will be demonstrating this weekend that he's able to execute arbitrary code on a 3.0 unpatched iPhone.

Leo: As we know, the crash is often a precursor to that; right?

Steve: Yes. Crashes are the way these things - exactly. You start by crashing it. Then you analyze exactly what happened and then realize, oh, if we put this binary as part of our packet, then that'll get executed. And as you said, Leo, I mean, it is - it's a connected computer. And there is nothing more vulnerable in the world than a connected, open computer that is able to execute code from the data incoming. And normally you're just going to display text when you receive an SMS message on the screen. Unfortunately, there's a way to get the phone to execute what you send. And apparently there's a site you can go to to disable some reception features of the iPhone. You can, like, turn off email something-or-others. I was scanning to understand the nature of this. But there is no way to turn off the phone's vulnerability to SMS. So Apple will be patching within the next few days.

Leo: I hope.

Steve: Rushing to get this thing done because the guy said, look, I'll give you until the Black Hat conference. But this is the title of my talk.

Leo: Now, Black Hat, there's really two conferences, Black Hat and then DEFCON.

Steve: Right.

Leo: One right after the other. Black Hat is like the hardcore, invite-only conference?

Steve: Well, and this guy is well known. His name is Charlie Miller. He wrote the "Mac Hacker's Handbook." He co-wrote it, and he's regarded as an OS X authority. So he had Apple's attention immediately. And he's, you know, it's serious business.

Leo: Wow. Yeah, no kidding.

Steve: So there's news on the iPhone.

Leo: But we just got - we don't know, and let's hope hackers don't know, the details until this weekend.

Steve: Yeah. And the good news is it sounds to me like you just can't randomly send a text message to it. You're going to have to go through some work in order to make this happen.

Leo: And you have to know the phone number, obviously.

Steve: And exactly, you have to know the phone number in order to...

Leo: Most everybody knows my cell phone number, so...

Steve: I was just going to say, I was surprised when you received a text message because I...

Leo: Well, you know, it's gotten out so many times it's not really a secret. And, yeah, oh, boy.

Steve: Yeah. Maybe you ought to turn it off, Leo.

Leo: The phone?

Steve: It's your phone, isn't it.

Leo: It's my phone. I can't turn it off.

Steve: That's a problem. Well...

Leo: Hey, if I'm hacked, I'm hacked. What the heck.

Steve: As far as we know, this is not in the wild. This one guy knows about it. He's acting responsibly. But he's told Apple, look, get your act together, get this thing patched. What's the patch technology for the iPhone? Is it able to, like, push patches out very quickly?

Leo: Yeah. Just like all cell phones, AT&T pushes it out and says - wait a minute. No, that's not true. I take it back. That may be a capability that AT&T has. But normally your phone is not patched until you hook it up to iTunes and synch it. And iTunes will then say, usually, there's an update. Do you want to apply it? It's really much more volitional. It's not - there's no automatic patch. Unless AT&T, you know, a lot of cell phones you have that automatic capability. Maybe AT&T does have that. I hope so. It's not just AT&T, though. You know this is a worldwide system.

Steve: The exact quote was "A bad SMS vulnerability that allows an attacker to remotely install and run arbitrary, unsigned software with root access."

Leo: Couldn't be much worse.

Steve: No.

Leo: Could not be much worse.

Steve: When you receive it in a text message.

Leo: Geez.

Steve: Yeah. Meanwhile, there is a zero-day exploit which is unpatched, zero-day meaning currently being exploited, of an ActiveX control for Microsoft's Office web components. There is no way around this. If you go to a malicious web page or you open email with an HTML viewer, your machine can be taken over. This is not a problem for people running Firefox. This is only if you're using IE. I use IE only to run Windows Update. So I'm safe. I'm hoping our listeners are to the point now where they're no longer using Internet Explorer, in which case they're not going to have a problem. The next Patch Tuesday for August I'm sure will cure this.

However, if you need to use IE, the only solution is to turn on the kill bits, the so-called kill bits for this ActiveX control. Microsoft has a page that makes it as simple as a single click. It's support.microsoft.com/kb - which coincidentally stands for kill bits. Also knowledge base, of course. So it's /kb/973472. So again, that's support.microsoft.com/kb/973472. That'll take you to a page that's got the new Fix me button on it, where you click it, and in doing so it runs some script which turns these kill bits on. Now, the kill bits, this is something where you're wishing Microsoft had done this the other way around. They ought to be enable bits for all these ActiveX controls, which are normally off.

Leo: Right, right.

Steve: This is like...

Leo: Default to off.

Steve: Yes. This is like the old days of the firewall, where the original firewalls were allow all, and then you blocked specific things. Well, that strategy didn't last very long. And everyone finally knows that a firewall should deny all and then allow only the traffic that you know you want.

Leo: Right.

Steve: Well, Microsoft got it backwards. And unfortunately IE with scripting allows any ActiveX control, even if it's not supposed to be, if it was never intended to be a web control, it's by default you can invoke it. So here's, you know, an Office component, this does happen to be a web-based component, an Office component that you probably don't need to use, you don't want websites to invoke, yet a bad one can. And due to the fact that there's a remote code execution vulnerability in it, it allows your machine to be taken over remotely. And it is now being maliciously exploited as we speak.

Microsoft has no fix for it. My guess is they're not going to do an out-of-cycle patch. They'll wait till August. So if you need to be using IE, and if you might be viewing email that you don't control, or you're going to websites that you don't trust, then turning these kill bits on for sure is a good thing. And after the patch you can turn them off again to get that functionality back. So again, I hope our users have moved to Firefox, and they're only using IE for running Windows Update, which is where I finally am.

Leo: It strikes me this is the most depressing show in history. Now I can't use anything. I can't use Firefox. I can't use my iPhone. I can't use IE. Can't use Windows. They all have unpatched, zero-day flaws.

Steve: It really is a problem. And it's funny because as a science fiction buff I've - we've all read stories like this where people like Neo from "The Matrix" are, like, selling on the black market some sort of disk that does something. And it's like, oh, come on. Aren't we going to solve these problems? It's like...

Leo: I think not.

Steve: ...there's no sign that we're going to. And I've got even more stuff, so. I do have some good news.

Leo: Oh, good, please.

Steve: Let's do good news...

Leo: Cheer me up.

Steve: ...for a change.

Leo: Okay.

Steve: Phorm - P-h-o-r-m - this for lack of a better term "heinous" marketing company, remember that we did a whole episode on the Phorm technology. These are the people who were installing their equipment in ISPs' facilities, intercepting all of the ISPs' customers' web traffic, and inserting their own cookies into - masquerading as cookies from every site that people went to in order to establish a comprehensive identity that was pervasive and pernicious and that you just couldn't get rid of.

Because British Telecom, which is the No. 1 U.K. ISP, did a test of this secretly, without notifying any of their customers, when the word of this leaked out, it caused a huge uproar. In fact, it turns out that the EU, the European Commission, has also begun to take legal steps against the U.K. government for its failure to take action against Phorm or BT for the two trials of the technology in '06 and '07, which they conducted without gaining customers' consent. So, I mean, this has become a huge political problem. British Telecom just formally announced that they are putting their work with Phorm on hold. The BBC reported that, upon that announcement, the stock value of Phorm fell 43.16 percent. And then...

Leo: Woohoo!

Steve: Yes, and then...

Leo: There is justice.

Steve: ...the No. 2 ISP in the U.K., which is an ISP called TalkTalk, they also announced shortly after BT did that they are dropping Phorm and pulling out of it. And that kicked the shares down to a total of more than half of its value lost. So it really, I mean, all of this bodes poorly for Phorm's future, which is one bright speck of news here in an otherwise gloomy podcast about security problems.

Leo: Just don't tell me the Kindle's been hacked, that's all. I just...

Steve: Well, there was a problem.

Leo: Oh, no. No, no, no. I was thinking, I'm just going to sign off the 'Net and read books. But I can't even do that now.

Steve: Well, you may find that the books you want to read are gone.

Leo: Oh, yeah. Isn't that an interesting story.

Steve: Yes. Amazon did something very controversial. No one realized that Amazon was capable of removing books from the Kindle. But Amazon can and did. What they're saying is that somebody posted two of George Orwell's books, "Animal Farm" and "1984," onto somehow like a - they had some unauthorized party posted...

Leo: Yeah, there's a self-publishing feature on the Kindle that I didn't know about, or on Amazon, yeah.

Steve: Right, exactly. And apparently people bought copies of "Animal Farm" and "1984" for just 99 cents, not super expensive, and many people noted that it was a little bit ironic that it was George Orwell's "1984," the Big Brother book, that was then - that was removed from Kindles when the actual owner of the copyrighted content notified Amazon. Amazon sent email out to people who had purchased it, saying, "We're sorry to notify you that this was put up on our site illegally. We have removed the content from your Kindle, and we're going to refund your 99 cents."

It caused a big kerfuffle because people were upset with the idea that they didn't really have - they didn't have, like, control over their content. Fred von Lohmann, who's a staff attorney for the Electronic Frontier Foundation, said, "There's an enormous difference between buying a book and buying a tethered media device," as he termed it. He said, "And this incident really underscores that fact. Consumers carry with them analog-world expectations." And then he said, "It's not clear from the Kindle license agreement that Amazon has the right to delete purchased content." He said, "I don't see that many loopholes." He notes that the Kindle license agreement states, "Amazon grants you the nonexclusive right to keep a permanent copy of the applicable digital content."

Leo: There you go.

Steve: "And to view, use, and display such digital content an unlimited number of times." And so he says, "Well, maybe the term 'applicable' is the out that Amazon would use if it came down to it, saying that, well, illegally uploaded content is not applicable to our license; therefore the users don't have the right to maintain it and keep it and view it an unlimited number of times.

Leo: Well, it may be moot because Amazon said, well, we're sorry, we'll never do it again.

Steve: Precisely. Exactly. Amazon said, well, in any event we've learned a lesson. I don't know what they'll do in the future. Maybe they would just pay the content holder the equivalent value. That would have certainly caused much less problems and concerns.

Leo: I came up with a solution, which would have been a good solution, which is to switch it for a legitimate copy. Here's the problem. Now, I don't know if this is confirmed. But according to the Times, students who had notes attached, who were using it for class, lost the notes.

Steve: Oh, right.

Leo: Now, that, I think, has to be illegal. I mean, that's got to be a violation because you're deleting my content.

Steve: Because it's the users' own content that they've added to it would then be lost.

Leo: And I haven't confirmed. I thought the notes were separate.

Steve: I would think they are. I think they are stored, well, certainly you can't be modifying the file. So it would be a file of...

Leo: A sidecar of some kind.

Steve: Well, it would be a file with pointers into the copyrighted content file.

Leo: So that might just break it.

Steve: Because it's all encrypted in DRM.

Leo: Right. In any event, thank goodness they're not going to do it again. Because...

Steve: No.

Leo: There's got to be a better way. I suggested that they send an email or they put it on the Kindle, they probably could do this, saying hey, you've got, you know, we found out this is not a legal copy. We'd like to offer you free a replacement copy of "1984" and apologize. And please delete it. I mean, that's all they can do, really.

Steve: For no additional cost. I mean, Amazon would eat the cost of however many copies...

Leo: Well, they did that anyway because they reimbursed people.

Steve: Well, no. They reimbursed them 99 cents.

Leo: Oh, they didn't give them the full amount?

Steve: No. Well, no. But that was what they paid.

Leo: Oh, okay.

Steve: They only paid 99 cents for this.

Leo: Oh, I see, yeah.

Steve: And so they reimbursed them what they paid. But imagine Amazon would say, you want this, fine. We made a mistake by allowing this to be purchased for 99 cents. You can now have the real one; or, frankly, just pay the copyright holder however many of the bad ones got downloaded.

Leo: There you go.

Steve: Yeah. In other news, older versions of McAfee have once again been destroying Windows. We talked about this the first time it happened in May, so not that long ago, where an update to McAfee's virus scan misfired, wrongly discovering a "worm," unquote, in valid Windows system files, quarantined them, and caused Windows to crash. And users could not get Windows to boot anymore because McAfee had said, no, these files are bad, you can't have them, they're infected, even though they were critical Windows system files.

Well, this happened at the beginning of the month, on July 3rd, obviously just before the Fourth of July. With McAfee's DAT 5664 update, many people found that their Windows systems crashed. And to me, Leo, this makes me just want Microsoft's Security Essentials solution for this all the more. We talked about that a couple weeks ago. Microsoft's in beta, 75,000 copies instantly downloaded. The reviews have been stellar, by the way. They continue to be stellar.

Leo: I love it.

Steve: No false positives. It updates as often as it needs to, maybe even as much as hourly in order to keep itself current. From Microsoft, integrated well into Windows, not being a bigger problem than the problem itself, which here again we see an example of McAfee being...

Leo: All the time, yeah.

Steve: Yeah. I just can't wait. I'm...

Leo: Well, it's going to change. I mean, McAfee and Symantec and everybody else are going to have to think of a new business. I mean...

Steve: Yes. They had a long time to make hay. And it was absolutely foreseeable. Just as it was foreseeable that Microsoft would add a firewall to Windows, it was foreseeable Microsoft would get into the antivirus / antimalware business themselves. And the good news is, it's just going to be free. It'll be the first AV that I ever run, and I'll run it everywhere, and I'll recommend it to everyone - unless there's any downsides that we learn about. And of course we'll let our listeners know either way.

Okay. Denial of service attacks on the U.S. and South Korean websites. On July 4th, which I guess coincided with North Korea's July 4th missile launches...

Leo: Right, and the day I arrived in China.

Steve: And the day you arrived in China.

Leo: Completely coincidental.

Steve: A not hugely damaging but certainly disconcerting distributed denial of service attack was launched by - there's been some dispute about the number of PCs. Some reports said 20,000. But a Vietnam research organization that found the command-and-control servers and tracked them back estimated the number was 177,000 infected machines. The U.S. Treasury Department, the Transportation Department, and the FTC all had their websites briefly taken down for various lengths of time. Some experts felt that this wasn't a high-strength attack; and that, had these organizations had better networks, had they outsourced them, for example, distributed them using Akamai so that there wasn't a single point of attack, they would have been able to stay up. I would imagine we'll see those kinds of changes come about as a result of this.

There were some bogus reports saying that this was actually triggered by or controlled by North Korea. But that was later debunked. What happened was, this thing was called W32.Dozer, which was actually a sort of a loose confederation of already known tools. There was this W32.Dozer that was a so-called "dropper" that contained all the other components. It was sent to users by email. So this was a worm. And the old Mytob agent that we've heard about before, W32.Mytob, that handled the mass mailing, gathered email addresses on the machines that it infected. So Dozer dropped Mytob on the system.

And then there was another trojan and a variation of MyDoom. MyDoom was what did the denial of service attacks on these machines. So there was sort of this collection that would land on the machine, brought in through email. If the user clicked the link to execute this Dozer, it would drop the other components out. One of them would be the backdoor zombie that would then use eight different command-and-control machines that were later found. And then another one of these components would rifle through the user's system, finding email addresses, and then mail itself out to all of the addresses that it could find in order to spread wormlike.

So that was on the 4th. What was then found, upon analysis of this, is that there was some weird self-destruct code which you typically don't see in these sorts of tools. There was a timer set to go off on July 10th. So less than a week later, only six days later, in a weird sort of way, it would search the machine for 30 common file extensions - .doc, .pdf, .xls, basically user content files - copy them into an encrypted file, and then overwrite the copied files, as if it was quarantining and encrypting and, like, sequestering these specific user content files from the machine's owner. Then it overwrote and blasted the master boot record on the drive, preventing the machine from booting.

So what was strange was that, after six days, basically it encrypted a whole bunch of files, it didn't destroy them, but it encrypted them and then prevented the machine from booting. So it's like, I mean, it was puzzling security experts. It's like, okay, well, what's the logic in this? It wasn't at all clear. Then four days after that, on the 14th, this Vietnamese security company that I mentioned, the Bach Khoa Internet Security, they tracked down eight command-and-control servers and then tracked down the single master server which was spreading its control out to those eight. And that server was located in the U.K. And that, again, uninformed press said, oh, well, this was based in the U.K. It's like, no.

Leo: No.

Steve: We still don't know. And as far as I know to this day there's been no confirmation of who was actually behind it. The U.K. machine was doubtless just one other machine that got taken over, and then it was the distributor to the eight other command-and-control computers. So that's the tune-up on what all these denial of service attacks were.

Leo: And we have no idea where it came from.

Steve: No, none whatsoever. I mean, which is not to say it's impossible because now that they found the machine in the U.K., if somebody tried to contact it again, then potentially you could track back. But all you have to do is run through, like, The Onion Router network, the TOR network, and then it becomes impossible to backtrack that. I mean, the TOR network, as we know, we did an episode on it, it's designed so that you can't backtrack the traffic through it.

Leo: Well, and a good hacker, I mean, we've known this for years, does in effect the same thing by going multiple servers and multiple layers.

Steve: Through proxy servers and, yes, exactly.

Leo: I mean, I doubt they use TOR. But they do something like that.

Steve: Yup.

Leo: By hand, yeah.

Steve: Yeah, they have a number of machines that they've compromised, and each one relays commands to the next one in the chain. And they're spread around the world, so it's virtually impossible to get cooperation from all governments and carriers in a short order. And it sounds like the whole thing was set to expire after a week anyway. So it's all sort of moot.

Leo: I wonder - and I wonder what the intent was.

Steve: It's just bizarre, yeah.

Leo: You've got to figure there was some sub rosa communication between the hacker and these governments, that there's something else went on. It's some sort of proof-of-concept kind of thing.

Steve: Yeah, it's like, okay, so why scan the machine for 30 different file extensions...

Leo: Yeah, that's weird.

Steve: ...encrypt the files and bundle them up. And then kill the machine.

Leo: Yeah, it's very strange.

Steve: It's just weird. It's like...

Leo: It's almost like a demonstration, really.

Steve: Yeah, or, like, maybe some of this, you know, they seemed to be using a bunch of other components, like so maybe there was, I mean, it could have even been inadvertent that it had this strange side effect.

Leo: Right.

Steve: One of the components had some behavior that the original designers didn't anticipate.

Leo: Sometimes these guys aren't really that bright. We may be giving them a lot of credit.

Steve: Yeah.

Leo: Yeah.

Steve: In an interesting little turn of events, we've been following the trial of the guys who were running Pirate Bay. And we know from talking about it before that they were found guilty of, not themselves of copyright infringement, but of essentially aiding and abetting the copyright infringement of the people who used their site. They lost a lawsuit, were sentenced to each one year in prison, and also had to pay a fine, or were fined, at least, 30 million kronor, which is $3.9 million.

Well, Pirate Bay has been purchased, was purchased by an outfit called the Global Gaming Factory, GGF, who paid $60 million kronor, not maybe coincidentally two times the fine amount, for Pirate Bay. What they've announced is they're going to go legit. And I read several accounts of what they had said, and some interviews. And I still can't figure out what it is they think they're going to do. They say that they're going to introduce models, economic models that ensure that content providers and copyright owners get paid for content that is downloaded via the site. And they say that they're going to - that it'll be a subscription service, so individuals, end-users, will have to - will pay some sort of monthly fee for access to the site. But if the users allow their machines to be used, and they also refer to if the users submit content, then they'll receive reimbursement for that and a reduction of the monthly fees. It sounds sort of screwy.

They also say that, like, ISPs that have really popular content sometimes get overloaded and can't deliver as much of the content as they want, so they're going to deploy some sort of peer-to-peer network in order to offload copyrighted content that ISPs would be providing. Some accounts say that these guys have had a year-long relationship with some ISPs on a basis sort of like this. So it's, anyway, it's not clear what they're going to do. But Pirate Bay is apparently going to try to go legit with some sort of model. Oh, and Kazaa, which is one of the earlier peer-to-peer networks, has said the same thing. They're going to be coming out with a legal commercial system, trying I guess to leverage their past popularity.

Leo: Hmm.

Steve: Weird.

Leo: Yeah. I don't know why it's worth 60 million. Kronor.

Steve: Kronor. $7.7 million.

Leo: I guess - do they have ads on it?

Steve: I agree, I don't know exactly...

Leo: How do you make money off this?

Steve: ...what it is that they think, I mean, certainly a huge percentage of the past success was that it was free. And I think as soon as you say, oh, look, we're the same Pirate Bay, but now you have to pay every month...

Leo: You're working with pirates. I mean, the people who use it...

Steve: Exactly.

Leo: ...are looking for free content. And there's plenty of free choices. They're not going to pay you any money.

Steve: Right, they're just going to go somewhere else. Instantly.

Leo: You've got the wrong audience.

Steve: Like, how fast can you click a different link?

Leo: Yeah [laughing].

Steve: Yeah, I agree.

Leo: Okay.

Steve: What is it that they think they're buying for their $7.7 million? It makes no sense.

Leo: Yeah. I think basing a business model on getting pirates to pay is not going to work.

Steve: [Laughing] Okay. So an interesting...

Leo: They have ads, apparently. We're showing our - we're showing we're just not with it and hip. They have ads on Pirate Bay. So maybe that's where they make their money.

Steve: Okay, well, I think the ad rates are going to drop, soon as they start...

Leo: The ad rates can't be worth that much in the first place.

Steve: Yeah. Goodness.

Leo: Who clicks a link on Pirate Bay? Oh, well, never mind.

Steve: Without holding their breath and being in a virtual machine.

Leo: Yeah, exactly.

Steve: And washing your drive afterwards. Okay. So there's a group called the Messaging Anti-Abuse Working Group, MAAWG, which not coincidentally is the acronym and the URL, MAAWG.org. They're sponsored by AOL, AT&T, Comcast, Cox, Yahoo!, Time Warner, Verizon, all the big names. They've put out a report which is formally titled "A Look at Consumers' Awareness of Email Security and Practices."

Leo: Oh, this is so depressing.

Steve: Or, quote, "Of course, I never reply to spam - except sometimes."

Leo: This was the most depressing stat of the week.

Steve: Okay. So a sample of 800 ordinary computer users in North America that this legitimate anti-abuse working group polled, 30 percent of these users said that they had clicked out of curiosity or mistake. 12 percent said they were actually interested in the advertised product or service. And 8 percent said they did not believe it was likely that their computers would be infected with malware and recruited for use in sending spam.

Leo: No, nobody would do that.

Steve: And so here's the problem, Leo. We've got somewhere there are 12 percent of people who are interested in having their penis enlarged, in having their mortgage refinanced, in whatever it is that spam is now selling. I'm a little bit out of the spam loop because, like John Dvorak, I get no spam any longer. I've solved that problem. So I don't know quite what is being delivered. But 12 percent of people say, ooh, and click on the link. Now, the problem is that the delivery cost of email is so low that 12 percent is, like, way more than there's necessary in order to make this spam economic model viable.

Leo: Oh, gosh, yeah. I thought it was one percent. And even one percent is plenty to make it viable because it's essentially free to send out millions of messages.

Steve: Yes, especially when you commandeer other people's computers and their spambots for you.

Leo: Right. So if you - what's the cost, you know, a fraction of a cent at best.

Steve: It's nothing. It's not measurable because it's not your bandwidth. I mean, it's...

Leo: Well, you would pay for the botnet, but that's, you know, $10,000 for, you know, infinite spam sending.

Steve: Well, okay. So I wanted to let our users know about this. If anyone's curious, there is a PDF you can download. I think it's, like, 67 pages. The entire content of this report is available and free and eye-opening. It's at MAAWG.org. And over in the right-hand column there is a link that is the - it's underneath - shoot, I had a note for exactly...

Leo: There's a Quick Links link.

Steve: That's it, Quick Links.

Leo: At the top, at least as we speak, it's the top item right there.

Steve: Yup, the top item under Quick Links over on the right is this PDF with some very disturbing stats because it looks like, you know, of 800 people polled, 12 percent said, "Yeah. I like spam."

Leo: I'm just shocked. I thought it was much lower than that.

Steve: Well, it means we're never getting rid of it.

Leo: Yeah. Oh, yeah. If it works, why stop? I always wondered. I thought, oh, how could this possibly work? Well, I guess I was wrong.

Steve: Meanwhile, late in June, in an interesting conference on cyber warfare that took place in Estonia, like a global group of people concerned about cyber warfare issues who are deeply involved in this, including two unnamed U.S. government officials, were discussing the pros and cons of proactive attacks. Two Ph.D. students at the University of Bonn in Germany have said that they've collected enough information about a quartet of well-established massive botnets that they could successfully attack and dismantle the malicious networks.

Now, we've talked about this many times, the fact that it is currently illegal for the good guys to be proactive, that is, we're only able to be reactive and to defend ourselves. We can't do anything else. Well, these two unnamed U.S. government officials said that they believe it is time to start creating policy in the U.S. that would allow for offensive cyber attacks. So we may be seeing this changing in the future. I mean, the problem is, essentially, the good guys' hands are tied. The bad guys have all the leverage. And even when security researchers know how to take down a net that is doing bad things, it's illegal for us to do so. Can't do it. So...

Leo: Oh. I don't understand that.

Steve: Well, I mean, the problem is that, if you modify someone's computer, even for what you regard as beneficial purposes, you've done so without their knowledge or permission.

Leo: But can't you take down the server?

Steve: Well, that's also somebody's machine. It's a much nastier machine, perhaps, but it's still...

Leo: It's doing something illegal. You could just go in and - I don't get it.

Steve: It's weird, though, that there are laws in other countries that are not even sure it's illegal.

Leo: Yeah. See, that's part of the problem.

Steve: Right.

Leo: Well, we've got to fix that. I mean, that's crazy.

Steve: I think it's being fixed. It's going to be slow. And again, we want to make sure we don't do the wrong thing because there's the possibility for abuse of these sorts of things. Right now we're clearly erring on the side of hands-off and hope for the best. But I guess, I mean, again, this seems to me like sci-fi. It just boggles my mind that there's, like, major cyber warfare budgets and teams and facilities, and everyone's starting to take cyber warfare very, very seriously.

Leo: Oh, yeah. Oh, yeah.

Steve: I mean, I know I sound nave about it, and certainly I'm not nave about what can be done and how. I guess to me it just seems so obvious that it's like, okay, well, fix your security. Fix your firewalls. Fix your iPhones.

Leo: Seems like we have ways to do that.

Steve: Yeah. Yeah. Exactly. And lastly, a group at Stanford, there's a Stanford security lab that will also be showing some very distressing news this weekend at the Black Hat conference. They tested 21 different devices from 16 different manufacturers. These are web-enabled gizmos - webcams, printers, network switches, photo frames, VoIP phones, remote management tools, all of these things - and, like, consumer routers, all of these things that are web-enabled, meaning that like so many peripherals now, they've got an Internet connection and a web interface. They tested the vulnerability of 21 devices made by 16 different manufacturers. There was not one that was not vulnerable to serious web-oriented problems. For example, they were able to enter JavaScript commands into the logon prompts.

Leo: Oh, boy.

Steve: And the device logged the log-on attempts. So when the administrator brought up the log, the act of displaying the log replayed the JavaScript commands, as it would because now they were in a web page because the log was web-based. And that allowed the commands to connect to a remote server and download malware. They said that among the worst devices were network attached storage devices. They enumerated five different classes of attacks, and they said that the NAS, the Network Attached Storage devices, were vulnerable to all five classes of attack. For example, you could rename files to JavaScript strings. There was no control over file naming in these. And of course we all have long filenames now in our state-of-the-art file systems. Well, long meaning JavaScript. And so anytime this device attempted to display the filenames on a web page, again, you were running JavaScript. So now there's scripting running in your directory listing, which is displayed on a web page, causing your browser to do whatever the JavaScript has said. And it's running in the local context. So even systems that have security saying don't allow remote sites to execute script, but of course we trust our self, well, now we can't trust our self.

Leo: Great.

Steve: All these devices have been put out and created with effectively no awareness of the security implications of having this kind of power on an easy-to-use, easy-to-administer device.

Leo: Hey, I've been looking at the iPhone hack that Charlie Miller's going to show this weekend.

Steve: Okay.

Leo: And it looks like it's for 2.2.1, which is the previous version of the iPhone firmware.

Steve: Oh, I didn't see that anywhere.

Leo: And he says that he hasn't, at least the articles I saw, doesn't know if it'll work with 3.0. Now, there are a lot of older iPhones still running 2.2.1. But it would sound like it would be a good reason for me, for instance, to upgrade my son Henry's iPhone to 3.0. And any new iPhone sold, of course, has 3.0 on it. Now, it's possible that this weekend he'll say it also affects - but he hasn't demonstrated it with 3.0.

Steve: Is Apple maintaining separate...

Leo: No. Not normally. You can keep 2.1 on your system if you don't agree to update. But the current version for all iPhones, all three versions of the hardware, is 3.0.

Steve: Okay. And so, and is there any rationale for people not going to 3.0?

Leo: Well, the reason Henry hasn't is because he - we jailbroke his iPhone. So any update will reverse the jailbreak, and he'll have to rejailbreak it. But I think we're just going to be doing that tonight. So any - it sounds like that's a reason to move to 3.0, you know, not noticing, not paying attention, having a jailbroken phone you don't want to mess with, there are a variety of reasons you might not want to move to 3.0. But it sounds like that's...

Steve: Right.

Leo: This might be the reason to do it. So it may, you know, I don't know if Apple fixed it in 3.0. Or I'm sure they fixed a lot of holes. And we won't know till this weekend.

Steve: Yup.

Leo: Very interesting.

Steve: So there's our mega security news update, my friend.

Leo: Wow. Wow. I'm trying not to be too glum here. At least Phorm got it.

Steve: Well, yes, yes, yes, yes, exactly. Phorm got what's coming to them. And everybody else is scrambling around, trying to patch holes.

Leo: Trying to patch holes.

Steve: Yeah.

Leo: You're right, you know, it just isn't getting better.

Steve: No, it's not. There's no sign that it's getting better.

Leo: Really interesting. And of course because now we know there's a financial, a strong financial incentive to hack systems, that's with 12 percent responding to spam, that's why you have seen all these exploits.

Steve: Yeah. There's a facility that was found and recently publicized called Golden Cash, which is a clearinghouse, run apparently by a group in Russia, where bad guys are able to go to the site and present credentials of some sort and purchase batches of bots that they want to exploit for various purposes. So, I mean, there's now a bazaar, essentially, a commerce system established for buying and selling bot fleets.

Leo: Well, remember we talked about the BBC buying that bot fleet for, what was it, 10 grand? It was cheap.

Steve: Right, right.

Leo: Cheap.

Steve: Right.

Leo: All right, Steve. Hey, boy, we got caught up. That's the good news. Next week we answer people's questions. Go to GRC.com/feedback to ask your questions. Actually for the next two weeks we'll have lots of Q&A.

Steve: Yup.

Leo: Of course GRC's a great place to go for SpinRite, the world's best hard drive maintenance utility. You've got to have it if you've got a hard drive.

Steve: [Indiscernible].

Leo: Yay. And all the free stuff Steve gives away all the time, like ShieldsUP! and Shoot The Messenger, DCOMbobulator, the Perfect Passwords. I actually put a link up on my Twitter account to an article about the Twitter hacks and whether your password might be susceptible, and the guy said, "Go to Steve's passwords page" - he mentioned your page specifically - "if you want a good password." Get a good password. That's GRC.com/passwords. It's a long password. It's not a memorable password.

Steve: No.

Leo: But it's a good password. And we will do this all again next week. You can watch us do it live every Wednesday at 2:00 p.m. Eastern, 11:00 a.m. Pacific. And I don't know what it is Chinese standard time, but that's the time I'm on right now. And I'll get off of that by next week, I hope.

Steve: Get some sleep, my friend. Get your bio clock adjusted.

Leo: Thank you, Steve.

Steve: And we'll talk next week.

Leo: See you then.

Steve: Thanks.