ISP Privacy and Security

Description: Steve and Leo discuss two new 0-day Internet Explorer vulnerabilities (both now being exploited on the Internet); then they explore the commonly expressed privacy and security concerns presented by the need to trust Internet Service Providers (ISP).

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-061.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-061-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 61 for October 12, 2006: ISP Privacy.

Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com. And by Dell. For this week's specials, visit TWiT.tv/dell.

It's time for Security Now!. Steve Gibson is here; and I have a report on my experiences with Windows Vista and Parallels on the Mac, and I'll tell you about that because I promised a review. But we have lots to talk about, including some security – oh, some security issues.

Steve Gibson: What do you know.

Leo: On Security Now!.

Steve: So tell us about Vista.

Leo: You know...

Steve: And Windows, Parallels.

Leo: I use Parallels. And in fact I'm just now downloading the final update to Parallels

because we've been in a kind of a beta. And the first beta did not run Windows Vista at all on my – now, I'm running on a Mac Pro with very high-end hardware, including a Radeon X1900 card and dual Xeons and so forth.

Steve: Well, in fact, I saw a mention in Jerry Pournelle's most recent column that you've got some – you have, like, a quad core system?

Leo: It's, yeah, basically. It's dual Xeon, so it's got four processors. And, boy, it runs – I mean, I have to say it seems to run at completely normal speeds. A little couple of weirdnesses, which I'll see if they fixed in the beta. For instance, sometimes I'll start it up, and it'll say, oh, the virtualization bit isn't set. And then the fix is to put your Mac to sleep and then wake it up, and for some reason that magically fixes it. And then the virtualization bit'll be set. You know, and the Intel processors. And that does make a significant difference in response. When everything's running as it should, and I'm running it with a gig of RAM – I have four gigs on the machine, but a gig of RAM dedicated to Windows.

Steve: Right.

Leo: It feels pretty good. We did some benchmarks at Call For Help. Sean Carruthers – because I had wondered how well – would it be better to run Photoshop in Parallels or run it natively on the Mac. And it actually is faster to run it as a Windows application in Parallels than it is to run it on the Mac. It's pretty slow on the Mac.

Steve: Very cool.

Leo: Yeah. Although fastest still would be to run it in Boot Camp as a native Windows application. Parallels is pretty good. I have to say I don't feel any urge to launch Boot Camp. Now, there are some people say – there's some question about whether I'm getting Aero Glass or not. I thought I was because it looked so pretty. But I haven't found a definitive – I'm a little concerned that I might not be getting Aero Glass, the high-end visual system. So I'm downloading the latest version. Maybe as we talk I'll install it, and before the end of the show I might have an update for you on whether I'm running Aero Glass or not.

Steve: Well, and in fact, on your Mac you probably have some humondo hard drive; right?

Leo: Yeah. I have a – I bought a, you know, it came with a 250-gig hard drive. But I am wont – I've done this on all my most recent machines – to go out and buy a Western Digital Raptor, which is a 10000-rpm hard drive, and use that as the boot disk. So that's a 150-gig or 170-gig boot disk, and then I have a 250-gig kind of secondary disk.

Steve: So unless that was, like, really full, you could certainly slice it down a little bit and use Boot Camp. I'm just thinking it would be useful, perhaps, to run...

Leo: Should I do a benchmark?

Steve: Well, or, well, just to, like, you know, for you to actually have a bootable – native bootable Vista.

Leo: Right.

Steve: Certainly at some point in the...

Leo: Certainly there's plenty of room.

BOTH: Yeah.

Leo: Yeah, that's a good point. Maybe I will do that. And there's some report that you no longer need Boot Camp to actually get Vista to boot on the Mac, which is kind of interesting. So I'll have to take a look at that, as well. I guess...

Steve: Wow.

Leo: Maybe Vista now supports EFI, or there's some black magic somebody's able to do. I'm not sure what it is, but I'll...

Steve: It certainly is sounding like Microsoft may be moving more toward running Windows on Mac hardware, which...

Leo: Why not?

Steve: ...would be – exactly.

Leo: Sells more copies. But to just, you know, to follow through on our virtualization conversation of the last few episodes, it really is a great way to go. I just don't feel any urge to install Vista anywhere else. It's still a beta; right? And why take the chance, when I can run it perfectly well on a virtual machine.

Steve: Right, right.

Leo: Really feels good. So yesterday was the Patch Tuesday, the second Tuesday of the month. Microsoft shipped a few patches.

Steve: Oh, a few. In fact, I've read it described on the web as a "hailstorm"...

Leo: That's probably not the word they wanted to use, but I understand where they're going there, yeah.

Steve: ...of patches. So, and they fixed another 0-day vulnerability which we haven't talked about before. It's different than the vector markup language vulnerability that, you know, we talked about several weeks ago. This one was – actually it was known since July, the middle of July. And then only a few weeks ago the infamous HD Moore, who creates the Metasploit framework, added full remote execution, you know, remote code installation technology to the Metasploit exploit framework for this vulnerability. It's – for months it was only known as a denial of service, meaning that it would crash your browser. But – oh, and I should explain that this was – I'm looking for what this – there's so many of them now, because there's another one I'm going to talk about, too. I don't want to get myself confused. Oh, it was a – there was a set slice method in what's called the web view folder icon function. And so for a long time all that anyone could do was get it to crash your browser. But of course any time you have a crash, that says, you know, some code ran that shouldn't have. And so once the black hat hackers figure out how to get the code they want to have run, run instead, it won't crash, it'll do something nasty. And it has been found in the wild installing rootkits on people's machines.

Leo: So that's kind of what you'd expect. The first time that they jump into code, it just crashes things. But they know how, well, hey, we're able to get it, and so we just have to figure out where to put our code so that it'll run it instead of just crashing and...

Steve: Right. And in...

Leo: It's just a first – it's a precursor, I guess.

Steve: Yes. And inevitably, this was developed from a so-called, you know, browser denial of service, meaning it would just, you know, deny your browser. It would just crash your browser. It was leveraged into a remote code execution exploit.

Leo: Now, is this something Microsoft patched yesterday?

Steve: Yes.

Leo: Okay.

Steve: Yes. So the point is, you absolutely want to be running Windows Update, or you want to make sure that you've got the most recent patches. I should mention that, you know, many times our Security Now! show notes is just a page where I say, hi, I didn't have any links. Okay. This is going to be a link farm. This is a link farm episode. I'm going to have a whole page of links. So listeners will probably want to go over to the show notes for Episode 61. And as I mentioned last time, that's the third icon in the little summary box on the Security Now! page. Because I'm going to have a whole ton of links for different stuff.

Leo: A slew.

Steve: So the previous 0-day exploit, the VML exploit, that of course has been fixed. Then...

Leo: By the way, I apologize for all the Windows sounds. You don't hear them, Steve. But

I'm booting Vista, and it's making a lot of noise.

Steve: Well, whatever it's doing, it's not messing up our connection, so that's...

Leo: You don't hear it. Well, that's one of the advantages of having quad processors is I'm looking at the CPU usage, and there's 100 percent on CPU 1, but we've still got only 7 percent on CPUs 3 and 4, so I think...

Steve: Right.

Leo: I think Skype's got plenty of headroom here. I'm sorry.

Steve: I think so. You mean you're doing this on the system that I'm talk...

Leo: It's the same system that we're talking on.

Steve: ...that we're using?

Leo: Yeah, I know, I'm a crazy man. I know.

Steve: That's amazing.

Leo: Yeah. Well, it's a test.

Steve: Okay.

Leo: Think of it as a test.

Steve: Only a test. Okay. So the original VML exploit that we talked about extensively a month ago, that of course was fixed by an out-of-cycle patch a couple weeks ago. Since then, Microsoft has fixed another 0-day exploit. The reason I'm making sure we're clear on this is that there is still another one.

Leo: Oh, man.

Steve: There is one that is now known is being exploited, is in the wild, and it has been confirmed that yesterday's Windows Update patches did not fix it. Microsoft knows about it. There's a link about it on their page. They're doing their standard, oh, well, you know, we'll either fix it in a normal patch cycle or in an out-of-cycle patch, if, you know, depending upon customer needs is what they say. However, this thing is, once again, it's gathering momentum. And we can expect to see, you know, a much wider range of exploits.

Leo: It's a remote-execution exploit?

Steve: It's a remote-execution exploit. It's now in the wild. Microsoft knows about it. But yesterday's patches did not include a fix for it.

Leo: Oh, boy.

Steve: So who knows when we're going to get one. Now, one of the things that people are noticing, and I'm sure this is not a coincidence, you know, it's evolution, it's what you'd expect, is new exploits are appearing either on the day of Microsoft's patch or shortly afterwards because they're wanting to get as large an exploit window as possible before...

Leo: Oh, so they wait until...

Steve: Yes.

Leo: They're taking advantage of this one-month delay.

Steve: Exactly.

Leo: Oh, man.

Steve: So it's good for security IT people because they know when to anticipate a hailstorm of patches. On the other hand, by – I mean, and it's logical when you think about it. This is what the bad guys would do.

Leo: Right.

Steve: Is Microsoft says we're going to patch on the second Tuesday of every month. So exploits appear on that day when Microsoft doesn't – or maybe shortly before or shortly afterwards. But, like, clustered around there so that they have the maximum opportunity of catching Microsoft, you know, off cycle to create the most opportunity for getting their malware installed in people's machines.

Leo: Those sons of guns.

Steve: Well, once again, the neat guys at ZERT, the Zero-Day Emergency Response Team, they've got a goodie which will fix both the 0-day exploit that Microsoft just patched and this other one. The other one is a – it's a problem in the direct animation ActiveX control that IE naturally will use. It's been known since the middle of September, that is to say shortly after Microsoft's last patch cycle. The SANS Security Institute has some, like, some mitigation steps. They say, well, use an alternate browser. Which is like, uh, yeah. That's, you know...

Leo: Okay.

Steve: ...Firefox.

Leo: We've been saying that for a while.

Steve: Or Opera or whatever.

Leo: Right.

Steve: Or they say disable ActiveX scripting. And of course, you know, the way I run, as I've said before, is I've got my security tightened so that I can browse around the 'Net with no ActiveX, and then selectively enable it for sites where it, you know, there is some functionality that I need.

Now, there's another thing that can be done. And I've got, again, links to all of this on the show notes for Episode 61, this episode. There's a way to set a kill bit for ActiveX controls that specifically prevents Internet Explorer and the Explorer viewer window – so that also covers you over in Outlook – it prevents IE from being able to use that ActiveX control itself. Again, I've got a link to Microsoft's page that describes it. In order to do this, you've got to get in and muck around with the registry. So instead, that's what the ZERT guys have done. They've got a very clean GUI and command line versions of what they call their "ZProtector," which apparently is going to be maintained and evolved over time, the idea being that when something occurs that's 0-day, they'll quickly respond by making an easy fixer, you know, a 0-day protector that will, for example in this case, just enable the kill bits so that IE won't – it'll basically neuter that functionality in IE until Microsoft gets around to fixing it. Then people will have to turn that back on. So it's very much like what they did with the VML exploit.

This thing is available from ZERT. You could put ZERT into Google and find it easily. Or again, the show notes page at GRC for this episode has links to it. They provide full source code. I've looked over it. It looks fine, I mean, these are good guys. These are white hat hackers. And it looks like they're going to be real busy, not only now but almost certainly in Vista times, fixing these sorts of problems. Because, I mean, we've really got a new form of arms race going now where, exactly as you said, Leo, hackers are clustering their release around Microsoft's timing in order to maximize their window of opportunity. And it's now – the race is to install malware in people's machines in order to take them over for various purposes. And it's going to be a nightmare.

Leo: Wow. Well, I'm glad that ZERT's around, anyway. And it's interesting that hackers have – they're so adaptable that they quickly sense an opportunity and take advantage of it and, like, this one-month delay.

Steve: Well, and really, you know, it's the kind of thing where after the fact you would think, yeah, well, naturally that's what they would do.

Leo: Sure.

Steve: They want the most opportunity for infecting machines, so they're going to wait till

Microsoft does a cycle and then dump their new malware out on the 'Net. And so, you know, this, again, I do recommend people who are using IE, who normally have ActiveX enabled, those people ought to protect themselves. Again, I don't want to get alarmist about this. This isn't yet a huge problem. But Microsoft just missed the opportunity to patch it. It did not make it into this round, that is, yesterday's Windows Update patches. And who knows how long it's going to be. Microsoft may do another, like, you know, mid-cycle patch two weeks later, as they did two weeks ago for the VML vulnerability, or not. In any case, if you're a person who's using IE with ActiveX installed, and you tend to go around to, you know, the darker sides of the Internet, that's where this stuff is being installed and being used now to take over people's machines. Again, another 0-day exploit, the third we've talked about in almost as many weeks.

Leo: Wow. Anything else to talk about today?

Steve: I think that covers our errata.

Leo: All right.

Steve: What I want to talk about today is to sort of address – this is sort of almost a mini Q&A, just a one-question Q&A.

Leo: Oh, but what a question.

Steve: Well, it's a – yeah.

Leo: It's one we get a lot.

Steve: It's a good one. It's one, in fact, what I was talking to you about before we started recording, what I wanted to talk about. You said, oh, yeah, someone just asked that, you know, today or yesterday.

Leo: I did an interview today, and somebody called up and said, "Do instant messenger programs log the chats?" And I said, well, some do, some don't; but your Internet service provider may well be logging what you're doing online.

Steve: Right. And the question we get, that we get submitted on the form at the bottom of the Security Now! page, and I see it often, is, okay, I've got my computer secure. I've got, you know, WPA Wi-Fi, I'm, you know, I'm doing everything I can. But what are the concerns about what my ISP is doing? You know, and we could generalize ISP a little bit. Most people think of ISP, of course, from their home network, who is your Internet service provider. But, for example, in a corporate environment, your corporate IT people are the, you know, basically your conduit out to the Internet. What are the security implications of, you know, sort of the aspects that you don't control in your connection to the Internet. And it's a good question, of course, because certainly it's like, I guess, sort of a weak link in the sphere or area that an end-user is able to control.

And we can break this down into sort of two forms of potential vulnerability. One, I would say, is the sort of the real-time packet flow, exactly as you were saying, Leo, in your instant messenger example. That is, the idea that an ISP might themselves log, or even in some cases

be legally compelled to log, certain classes of traffic which are moving across their borders.

The second category, which is sort of different, related but different, is any sort of database or long-term storage, or even for that matter short-term storage. And the most prevalent category there is email because most ISPs provide the SMTP server that remote systems use for depositing mail into their server, which will then be picked up by your POP client or your IMAP client when you go to retrieve mail. And in exactly the reverse fashion, you tend to plant mail on that server, that SMTP server, which is then relayed out to the rest of the Internet. So that's, you know, obviously the way email functions. So there's both a concern of data flowing through the ISP and sort of this database or storage where you are explicitly depositing messages, either incoming or outgoing, in the form of, you know, email or any other sort of, like, static transaction.

So I guess the point of clarification, the idea that people want some sort of assessment of is, first of all, you know, what do they have to worry about? Well, anytime email is not encrypted between endpoints, it's inherently going to be in the clear. So, for example, even if you used SSL to create a secure connection to your ISP, SSL is encrypting your data in transit, but it's decrypting it at the other end, and it's going to be stored in the clear by the ISP. So there is a vulnerability there. If you're just using SSL to transfer your mail safely, it is not encrypted at the ISP, nor is it encrypted anywhere after that when it goes across the Internet and rests at the destination ISP prior to being picked up by a user.

Leo: Well, important to understand, that's if you're using POP mail.

Steve: Well...

Leo: If you're using web-based mail, like for instance Gmail with SSL, then that's encrypted, and the ISP never gets a look at it.

Steve: No. It's not encrypted.

Leo: It's not.

Steve: It's not encrypted at the ISP, nor when it goes...

Leo: Oh, okay. So SSL is only used for the log-in, not for the transmission.

Steve: Well, it is used for the transmission. And so it's encrypted in flight. But once it gets there...

Leo: Well, that's my point. Your ISP in that case is Google.

Steve: Right.

Leo: So your Internet service provider is not seeing that mail.

Steve: I see what you mean. Yes, that's absolutely true. It would be unencrypted when it rests on the destination server. And if that were Google, then it would be going through your ISP, and they couldn't see it at all.

Leo: Right, right. So...

Steve: Yeah, that's absolutely the case.

Leo: And there are companies like Hushmail, for instance, that maintain encrypted mail even at the server side. So, but you have to take extreme – you'd have to take these extraordinary steps to make sure that your email was safe. You'd encrypt it, basically.

Steve: Well, yes. And in fact that's where I'm headed with this, is that the – and we've talked about it in passing. But I wanted to, again, readdress the issue of PGP in this context because people who really want to know that they've got, you know, as it's called, Pretty Good Privacy, but when in fact this is like Really Good Privacy, of their email from the point it leaves their machine to the point it arrives at its destination, no matter what happens to it in the meantime, you need to use an extra tool like PGP, which is now freely available, is at PGP – or you use GNU PGP.

Leo: Yeah. In fact, the PGP Corporation is a commercial entity that currently owns the PGP code base. They make a free version, but it's – boy, you've got to jump through hoops to get it. And frankly I don't recommend people do that. They just use the open source version, which is, as you say, the GNU Privacy Guard, or GPG. And that's available from GNUPG.org. That's what I use. And it's PG, completely PGP compatible. It looks just like PGP. You store, in fact, you store your key on the PGP key servers. People can use PGP interchangeably with GNU PG – or GP. But – it's a little too many Ps and Gs here.

Steve: PGPGPG.

Leo: The problem is, I mean, I use it to sign my mail. And if somebody sends me a key, from then on all mail, all our transactions are encrypted in both directions. But most people don't use it, so most of my mail is still unencrypted, even though I have the capability.

Steve: Exactly. Well, and you know, I'm not a PGP user because I just...

Leo: I know. So I can't encrypt my mail to you, Steve.

Steve: Well, but, you know, we're just gossiping back and forth.

Leo: Oh, yeah, well, that's easy for you to say.

Steve: Well, and I think that's a perfect example, too, is that most people probably don't have this concern. But it's a question that is being asked continually. So I wanted to formally address it and just explain that, you know, email may be encrypted on the fly, but it is not encrypted once it arrives at your ISP's server, not is it encrypted – nor does it stay encrypted from then

on unless you do something like use PGP in order to provide real end-to-end encryption where all the server is then seeing is a blob of ASCII gibberish. They have no way of dealing with it. No one inline, I mean, no U.S. government subpoenas, no packet logging, nothing is ever able to decrypt that. So, I mean, it is really good security from point to point.

So the second class of concern is just this flow of traffic. And there's really nothing a user can do except be aware that an ISP, unless you're using an SSL connection or a VPN in order to tunnel through your ISP, anything you're doing is susceptible to their monitoring. Now, I mean, I don't want to get overboard and suggest that ISPs are monitoring. On the other hand, there has been evidence of and stories about the, you know, various factions in our intelligence services who, you know, FBI, CIA, NSA and so forth, that are doing monitoring of ISPs. And it seems to be something which is growing rather than decreasing.

Leo: Alberto Gonzales, our esteemed Attorney General, has asked ISPs to keep two years of information on everybody, just in case they need it later. So...

Steve: And of course that's...

Leo: That's voluntary, but...

Steve: It's been met with a huge amount of resistance by the ISPs because, you know, they first...

Leo: It's a lot of work.

Steve: Well, yeah. They say, who's going to pay for that? I mean, two years of all of their traffic is a phenomenal amount of data. And it's the sort of things like, okay, then if you've got this much, you know, data, how do you make any sense of it? How, you know, how do you find a needle in a haystack, literally. So you're right, there is an intent to diminish our privacy in this fashion. And again, PGP and using SSL connections through your ISP, or VPN connections, provide you with, you know, absolute state-of-the-art bullet-proof protection.

Leo: So if you're using other things, like, well, just surfing or instant messenger, there are encrypted instant messengers. When you're surfing with an SSL-encrypted site like your bank, you're safe.

Steve: Yes.

Leo: But the rest of it is just floating out there in the clear.

Steve: Yes. You know, for example, typical uses of Google, where you are entering data into a Google form, is not encrypted. So somebody can see what you are searching for. Of course, Google knows; and they are, we know, building up stats for whatever purposes, they say in an anonymous fashion. But in the case of your ISP, your ISP with whom you have an account knows who you are, knows your identity, knows, you know, everything they need to know if somebody was making them, or for whatever reason they were choosing to associate your traffic with you, they have the ability to do so. So, yes. Anytime you are not using SSL for web browsing, all of the data, the URLs you go to, the data you enter into non-secure forms, you

know, pretty much anything you do on the 'Net is being passed back and forth through your ISP in a way that can be examined and filtered. So essentially that's the answer to the question that we get so often.

Leo: And the news is bad.

Steve: Well, yeah. Again, it's, you know, you and I don't use encrypted email because we're just generally...

Leo: Because you don't. Because I would. If you used PGP, we would have encrypted email.

Steve: But, yes, but there's nothing we're talking about that...

Leo: Ah, but the point is that if everybody did it, then there would be no obvious – you see, right now if I sent encrypted email with some people, the presumption is, well, look, he doesn't encrypt anything except for these few messages. We ought to look into this. If all of my streams were encrypted, and if everybody did the same, there'd be no way to say, hey, this one's suspicious.

Steve: Right. Well, and in fact...

Leo: So, Steve, install GPG, would you please, I beg of you. I do have – it's funny, there are a number of people, since we've talked about this so many times now, there are a number of people who use me as a test, saying, can you read this, am I getting my key and so forth. And I've responded to them. The people who have uploaded keys to the key servers, I've downloaded the keys. And every time now we exchange email, it is automatically encrypted. I don't see it. It's, you know, it's painless on my end and their end. We don't really see anything going on. But in fact it's automatically encrypted. It's a very easy thing to do, and I think a very good thing to do.

Steve: Well, okay. Looks like maybe – maybe I'll have to take a look at that.

Leo: You don't have to. I understand. Your point is that why bother. And I think a lot of people...

Steve: Right.

Leo: ...feel that way. But I think that, until everybody kind of uses it routinely, any use of it is then suspicious. And so, you know, there's a reason why it would be nice if everybody used it.

Steve: That's a very good point.

Leo: Yeah, yeah. But honest, Alberto, nothing's going on here. There's nothing, I mean, nothing to spy on. Move along. These are not the droids you want. All right, Steve. I think we've wrapped it up; yes?

Steve: Yup, that was the answer to the question...

Leo: That great question...

Steve: ...that we're being asked so much. I've got a couple things on the burner that people are going to, I think, really enjoy. We mentioned last week this MojoPac utility...

Leo: Yeah.

Steve: ...or product. It looks very interesting. I've opened a dialogue with the MojoPac guys because I want to understand exactly what they're doing. What it looks like they're doing, and it's hard to divine from their website because it's mostly talking about features and benefits and, oh, this just does everything, you know, that you could ever want. It's like, okay, but I need to know how and exactly what in order to know where the security and privacy, you know, boundaries are. But what it appears to do is essentially to use the facility in Windows for creating user profiles, and it allows you to make a completely portable user profile where all your applications and your data and other stuff is kept on a removable device. Which is – it's very cool. The problem is, they must be doing more than that in order for their claims to be valid. So I'm going to – I hopefully have a dialogue going with them. And I hope to have a complete presentation for Security Now! #62, next week's Security Now!...

Leo: Oh, good.

Steve: ...to, you know, really talk about definitively what this is and what sort of a solution it represents.

Leo: And just to wrap up my discussion of the Parallels solution, I don't have benchmarks. And I've love to get some, and I probably will do some. But RC2 is running under the current edition of Parallels. There are a couple of little things that I'm not crazy about. One is, in fact, it doesn't look like I'm getting Aero Glass, and I think that's because, try as I might, I can't get Windows to assess my hardware. And until it assesses – you know, because it's running in a virtual machine. Until it can do that, it can't really decide whether to run Aero Glass. I've tried the various – there are a couple of registry hacks that supposedly will make this possible, but none of them seem to work. So, but it does run fine, and it seems to run at nearly full speed. Until I get benchmarks, I can't prove that. But it's certainly usable. And boy, it's great, a great way to run a beta operating system. And that's pretty much it. I recommend Parallels. And I will install a Boot Camp, and then I'll be able to get Aero Glass and all the other cool features, I'm sure.

Steve: Right, right.

Leo: All right, Steve. We'll wrap this sucker up in record time, ladies and gentlemen. I

hope you've enjoyed this edition of Security Now!. Remember, it is sponsored, as it has been now for almost a year, by the great folks at Astaro Corporation. They make the Astaro Security Gateway. If your small or medium business network needs superior protection from spam, from virus, from hackers, as well as complete VPN capabilities, intrusion protection, content filtering, and an industrial-strength firewall, all in one single easy-to-use high-performance appliance – my 120 is about the size of a router, and it does all of that – contact Astaro.com, or call 877-4AS-TARO. You can schedule a free trial of an Astaro Security Gateway appliance in your business. If you're a home user, a non-commercial user, you can also download the software version of ASG for home use, run it on any PC, at Astaro.com. It's open source software, very powerful. You can even, if you want, subscribe to all of those additional features, running it on your hardware. It's very affordable. Astaro.com.

Also thanks to Dell. They are also a sponsor of this podcast and TWiT and Inside the Net. And we invite you to visit – I finally – I broke down. Dell's been giving me these, you know, great bargain computers to highlight on the Leo's Picks page. And I said, you know, these are all great, and the prices are remarkable. But I've got to say, this is the one I want. It's the Dell XPS 700. Let me – just check it out: TWiT.tv/dell. That's the one, configured as I want – in fact, it's my next computer for using for – we record and edit the shows on a Windows PC. You know I'm a Mac user for many things, but on the recording and editing I use a Windows PC. And I need a – I want a nice fast one. And Dell's got it, the XPS 700. Check it out: TWiT.tv/dell. And if you're in the market for a new computer, or you're going to buy a new Dell, do us a favor and go through that page so we get credit for it. TWiT.tv/dell.

Steve, it's been another great episode of Security Now!. Next Thursday we'll have another one.

Steve: Absolutely.

Leo: I hope you have a wonderful fall afternoon in beautiful Irvine.