Cyber Warfare

Description: Steve and Leo discuss the interesting topic of state-sponsored Cyber Warfare. While born through the imagination of science fiction writers, the reality of international, inter-nation cyber combat is fiction no longer.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-082.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-082-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 82 for Thursday, March 8, 2007: Cyber Warfare.

Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com. And by Nerds On Site. Looking to grow your IT service business? Find out how Nerds On Site can help. Visit Iwanttobeanerd.com.

Time to talk about security, protecting yourself, your computers, your home, your family, and our national borders with Mr. Steve Gibson. I kind of blew it up a little bit bigger than it really is. It's just your computers.

Steve Gibson: Well, actually we are going to talk about national borders today.

Leo: Oh, really. Oh, good.

Steve: Yeah, we're going to talk about state-sponsored cyber warfare.

Leo: Holy cow.

Steve: Which I think is, you know, a really interesting topic. And there's actually more going on than people might guess. So I think it's going to be really interesting.

Leo: Can't wait to hear that. Anything that we want to clear up from last episode or...

Steve: Oh, yes. The challenge of secure Wi-Fi just never seems to be resolved. We of course talked last week, following up from the week before, last week we were talking about this problem of how ad hoc networks, as opposed to infrastructure networks, an infrastructure being where you've got a base station you're connecting to, an ad hoc network being where you just have two random, for example, laptops that are able to directly connect to each other or associate in order to create a connection, and how unfortunately Windows XP is a little misbehaving. In fact, you had that neat anecdote from two weeks ago, Leo, about how there's sort of almost a virus, this Free Wi-Fi network virus that jumps from laptop to laptop.

Well, hearing last week's episode where we talked about and showed on the show notes page how to go through and deliberately disable this sort of automatic ad hoc network connectivity, some sharp people over in the GRC newsgroups picked up and said, hey, Steve, did you forget about the Windows Client Update from late last year? And it's like, uh. Then of course it rang a bell, and I remembered being aware of it, but it's something we definitely want to talk about.

Okay, now get this, Leo. This is really annoying. A completely patched, like right up to date, XP system that includes wireless will not have a client update to the Windows – it goes by various names, like Wireless Zero Configuration, WZC. But it will not have a really important update which all XP Service Pack 2 people will really want to incorporate. So it's something that Microsoft – it turns out it was on October 17 of '06, so only a few months ago, that Microsoft released this to fix a whole bunch of holes in this Wireless Zero Configuration. But they never put it on their list of stuff that you'd like to have automatically downloaded into your machine.

Leo: Oh, so you have to specifically request it.

Steve: Yes. Yes. And it's really important. For example, reading from – and on our show notes page, of course, I've got links to all this. But reading under Changes for Ad Hoc Networks, it says, "On a computer that does not have the wireless client update" – which is what we're talking about – "installed, wireless auto configuration" – which is the other name it goes by, either zero configuration or auto configuration – "automatically tries to connect to all the wireless networks in the preferred networks list that have previously been connected to." Get this. "If no infrastructure mode networks are present, wireless auto configuration sends probe requests out to try to connect to the first ad hoc wireless network in the preferred networks list. An observer could monitor these probe requests and establish an unsecured connection with a Windows wireless client."

So literally, a laptop that someone's just carrying around with them, when they're not connected into a network already, every minute it's sending out probes announcing networks that it used to be connected to or had been connected to in the past to see whether there might be a non-broadcasting network, that is, a network which is not broadcasting its SSID, its network identification, that would allow then this machine to connect to it. So it's, literally, it's spilling the beans. It's sending out the names of networks that your laptop knows about. So...

Leo: Wow. Wow.

Steve: Yeah. And so, like, okay. This is not a huge security problem. But who wants their Windows machine sending out, you know, by radio, Wi-Fi names of...

Leo: Here's people I trust. Here's people I trust. Okay, just come on, pretend you're one of them.

Steve: Yeah, I mean, essentially, anyone passively sniffing Wi-Fi packets will be learning about the names of the networks that the people around them have connected to in the past.

Leo: I would guess that's how the Free Public Wi-Fi...

Steve: That's exactly how it happens, is that a machine that has it, broadcasts it. Another machine says, oh, and connects to it. And now it has it. So the changes, on a computer that has the wireless client update installed, "Wireless autoconfiguration does not send probe requests to connect to newly created ad hoc wireless networks in the preferred networks list. Because many ad hoc wireless networks are created for temporary wireless connectivity" – I mean, that's like all what you'd be using it for – "you must use the Choose a Wireless Network dialogue box to manually initiate a connection to an ad hoc mode wireless network."

Okay, now, that makes sense. So here's a perfect example of Microsoft still not getting this tradeoff between privacy and security and convenience. Because the original design, even post-Service Pack 2, I mean, this is just in October, at the end of '06. So even post-Service Pack 2, the big, much-heralded security update for Windows XP, they're saying, oh, it's better to err in the direction of convenience and, oh, look, it just works, than it is towards privacy and security.

Leo: Interestingly, though, this whole Wireless Zero Config, while I guess on the surface it looks more convenient, it's caused more problems for more people. It is not, it is the opposite of convenient. I get people complaining all the time that they drop connections, and often it's because Wireless Zero Config is kind of promiscuous.

Steve: Ah, well, actually that's also one of the things that this update deals with is, if you end up with another network acquiring a stronger signal than the one you've got...

Leo: It just flips right over.

Steve: Yes, it's able to jump networks and switch to the stronger one. It's like, no. That's not my network. This is not a cell phone, where I want to be jumping between cell towers. So anyway, they've fixed a bunch of things. We've got links on the show notes page to this description, to the page you can use for downloading. And just I was curious. So I, literally, I took an XP machine that had never – it was fully patched, up to date. I looked at one of the main files, which is wzcsvc.dll. So that's going to be Wireless Zero Config service dot dll. On a completely patched XP SP2 machine, its file date was 6/21/05.

Leo: That's completely patched with critical patches, but not these optional patches.

Steve: Well, no, everything that – no, not, I mean, everything that you can get automatically from, you know, as you install XP, then you go through all the Windows Update cycles over and over and over until it finally, you know, the patches have had their patches, and they've had their patches. so that it's all settled down, and so okay, you've got everything you need, this thing is not part of that. And so only if you deliberately update, then it jumps you from a 62105 to 81806 on basically a whole set of files, which are enumerated on this page. So people will be

able to look at their files, see whether this has been done for them by someone, and most likely it hasn't been since it hasn't been that long ago, it was in October.

Leo: I'm sure mine's not.

Steve: And so everyone listening is going to want to run this patch because this basically locks down the wireless service, you know, this autoconfig sort of promiscuity of XP.

Leo: So once again, you'll run Windows Update. It's not a critical patch, though. You have to go in the optional patches. And what's the name of it?

Steve: No no no, Leo. It's not in Windows Update. You can't find it there.

Leo: It's not even there?

Steve: No. You have to deliberately go and ask for this by name.

Leo: Oh, grumble, grumble, grumble.

Steve: So the only way to find it, I mean, if you put in, for example, to Google or to Microsoft, you put in "wireless client update," I'm sure you could find it on Microsoft's site that way. So "wireless client update," put it in the Microsoft search box, I'm sure you'll find it. Or we've got links to it on our show notes. But there is no way, I mean, it doesn't show at all through any of the normal, you know, take-care-of-me-Microsoft updates.

Leo: It's not even an optional update. Okay.

Steve: Right.

Leo: And it is the first Google result if you do "wireless client update." And there's a download link on that page.

Steve: Perfect.

Leo: And that's for XP. Now, presumably they fixed that in Vista.

Steve: Yes. Given, you know, they know they made a mistake, and they should have fixed this; and Vista came out, you know, only last month, in February. We can presume. Although I have to say I'm still scratching my head about where they've hidden all these things in Vista. It's like, I dug around and couldn't find sort of the same thing that I'm used to seeing in XP. So...

Leo: This modifies six different files. So it's quite a big update.

Steve: Yes, basically it's the entire collection of Windows Zero – the Wireless Zero Config set. And I only read one aspect of the behavior changes. There's...

Leo: There's a lot of them, I see, yeah.

Steve: ...five or six different things that this thing says, uh-oh, this is really not what we want to do. And who wants their unconnected laptop, that probably has its Wi-Fi still on, the Wi-Fi radio still on, unless you're, like, really conscious of that, as I am, for example, to shut it down to save battery life, when I remember to do that, you know, who wants it broadcasting the name of networks it knows? That's just not cool.

Leo: Well, in the past we've gotten this question a lot on the radio show. And I just told people, disable the Wireless Zero Config service, that you don't want it because it's a bad thing. But now I have something better, which is download an update. And you know what, you should come on the radio show and tell everybody because I think people need to know this. This is something we want to get out very widely.

Steve: Ah, that's a great idea.

Leo: Any other updates?

Steve: Well, no, except that I've been trying to read this one really neat piece of email that we received about SpinRite saving someone's business? But, you know, of course last week it saved your computer, so I was quite willing to have you talk about that.

Leo: You do it now.

Steve: Anyway, so this is from – this is email from a Michael Diaz in New Jersey. And the subject of the email was SpinRite saves a business. He says, "I just wanted to drop you a note thanking you for your great product, SpinRite. I am a network administrator, and I use SpinRite on a regular basis to diagnose problems as well as refreshing drives on our older PCs. I'm well aware of the value and power of SpinRite as a business tool. That's why it's what I used when a friend's business was on the line." He says, "I have a friend who is an automotive specialty tuner." I didn't even know about this kind of thing. But he says, "He builds and customizes primarily late model Ford Mustangs. Many of these cars have 400, 500, even 600-plus horsepower. And in order to reliably and safely drive these cars on the street, there needs to be a very good tune, as he calls it, built into them. Modern cars are tuned via software. And that usually requires a laptop and a lot of tweaking to the car's software.

"So I receive a frantic call from a friend one day, basically saying his laptop will not boot, it starts up, gets a Blue Screen of Death, and then reboots, getting caught in a cycle. I know this is never a good sign, so I dart out to his shop with only SpinRite in hand. When I arrive there, my first question is, of course, do you back up the data on the laptop? To which I hear the reply, uh, no." So this ends up being, like, critical stuff for this guy. He says, "Knowing full well that his reputation as a tuner and the hard hours of work he's put into building his business are on the line, I put SpinRite to work. The first thing I notice is that the hard drive is clicking." He

says, "That is never a good sign. I start to wonder if I'm too late, but I continue on with SpinRite. It does not take long for it to find some bad sectors, and we decide to leave it running for a while. Many, many hours later, the scan finishes with a plethora of red Us showing on the screen. The only way I can describe it is, it looks like virtual Swiss cheese. As I attempt to reboot the laptop, the clicking is gone, and Windows boots."

Leo: So the red Us are unrecoverable sectors in SpinRite.

Steve: Yes. What it really represents is we were unable to get all of the sectors' data back. One of the very coolest things about SpinRite that makes it completely unique as far as I know is, we are able to read most of a sector, even if we can't get it all. And so SpinRite will try like crazy to get it all, and in fact that's what this whole DynaStat thing is, the Dynamic Statistics, is it's able to accept whatever the computer is able to read, even if it's not perfect, knowing that it's not perfect. And so it's very often the case that we can get one good read. But if not, even after trying a lot, SpinRite is able to say, okay, I couldn't get it all. But for example, out of 4096 bits, which is what a sector is, it might get 4090, which you could argue in many cases, for example, if it's a critical, for example, a file system sector, you might get back your file system because that one sector was preventing the whole file system from functioning. So you can tolerate some fuzziness in some sectors.

Anyway, so he says, "I attempt to reboot the laptop. The clicking is gone, and Windows boots. Not trusting the drive, I quickly retrieve his data and tuning files, as well as his custom tuning software, none of which he had copies of. Not long after transferring all his vital data off the system, the click is back. This time the drive just dies. Luckily, SpinRite was able to make it stable enough for me to get all the data off before it completely seized. SpinRite does not have to completely fix a drive to save the day. In my case, it did enough for me to get the vital customer data off the dying drive and, yes, save his business. I can't tell you how competitive the custom tuner scene is, especially in the world of super high-power street cars. One's reputation is key, and in this case that reputation is intact, thanks to SpinRite."

Leo: So the moral is here, back up.

Steve: Yes, please, please. I mean, I'm glad we're able to, like, come to the rescue in these cases. But really, when there's this kind of data – I'm sure his friend now has learned a lesson by seeing how close he came to the brink of losing everything.

Leo: He's very lucky.

Steve: And it generally takes one of those lessons to, you know, get someone clued in.

Leo: Unfortunately, it's really true. Hey, we're going to get to our subject, which is, I think, very interesting, cyber warfare, in just a second. We do want to thank Astaro, our sponsors for this show. They've released Version 7 of the Astaro Security Gateway, and a number of improvements, including, as we've mentioned before, transparent email encryption and decryption, which means it's centralized in the Astaro Gateway, so your users, your employees don't have to even know about it. No additional encryption software is required on their computers. It just does it all for them. It even handles digital signatures based on S/MIME and OpenPGP standards. Really, really works. And inbound mail is automatically decrypted. So it allows you to have a completely secure email without any effort on your part. Of course there's lots of other new features including SSL for VPN. In fact, I think the

Astaro is the only UTM appliance on the market with such an amazing array of VPN and remote access solutions. You can cluster them, which means it'll scale to any size. As many as

10 gateways can be clustered together. And they have, and this is for home users great news, eliminated the home user fee. So you can continue to download the home use package for free, as always for noncommercial use. But now you'll also get the base license, all subscriptions, and Astaro Up2Date for free. They're giving it away. So if you've got an old beige box lying around you want to turn into a security gateway, this is the way to do it. Astaro.com. And don't forget, you can call Astaro for a free trial in your business. Just call 877-4AS-TARO. We thank them for supporting Security Now!.

Cyber warfare. Even the name sounds scary. It sounds like "War Games." Sounds like Matthew Broderick should be part of this.

Steve: Well, yes. And I think the really interesting thing is that, without specific details, it's so easy to pass off this whole concept as just sci-fi. It's like, oh, yeah, come on. Like, you know, state-sponsored cyber warfare.

What I want to start with here is reading a really interesting article because it provides this kind of grounding and foundation. This was in Federal Computer Week. The article is dated February 13, so less than a month ago, from Norfolk, Virginia. The article reads:

"At the Naval Network Warfare Command" – okay, so first of all, there is something we have in the United States called the Naval Network Warfare Command."

Leo: Napoleon Solo should be an agent for that. My goodness, wow.

Steve: It says, "U.S. cyber defenders track and investigate hundreds of suspicious events each day." Oh, I forgot to read the title. The title of this article is "Cyber Officials: Chinese Hackers Attack Anything and Everything."

Leo: Yeah, that I know.

Steve: Is the title. So it says, so "cyber defenders track and investigate hundreds of suspicious events every day. But the predominant threat comes from Chinese hackers, who are constantly waging all-out warfare against Defense Department networks, Netwarcom officials say."

Leo: I don't know if they're targeting Defense Department networks because they're also waging all-out warfare against my website. So I think it's just general.

Steve: Yes. Well, it says, "Attacks coming from China, probably with government support, far outstrip other attackers in terms of volume, proficiency and sophistication, said a senior Netwarcom official, who spoke to reporters on background February 12. The conflict has reached the level of a campaign-style, force-on-force engagement, he said." I'm not even sure what "force-on-force" means.

Leo: Doesn't sound good.

Steve: Doesn't sound good. Then he says, "'They will exploit anything and everything,' the senior official said, referring to the Chinese hackers' strategy. And although it is impossible to confirm the involvement of China's government, the attacks are so deliberate, 'it's hard to believe it's not government-driven,' the official said.

"The motives of Chinese hackers run the gamut, including technology theft, intelligence gathering, exfiltration, research on DOD operations and the creation of dormant presences within DOD networks for future action, the official said.

"A recent Chinese military white paper states" – okay, get this. "A recent Chinese military white paper states that China plans to be able to win an 'informationized war' by the middle of this century. Overall, China seeks a position of power to ensure its freedom of action in international affairs and the ability to influence the global economy, the senior official said.

"Chinese hackers were responsible for an intrusion in November 2006 that disabled the Naval War College's network, forcing the college to shut down its e-mail and computer systems for several weeks, the official said. Forensic analysis showed that the Chinese were seeking information on war games in development at NWC, the official said.

"NWC was vulnerable because it was not part of the Navy Marine Corps Intranet and did not have the latest security protections, the official explained. He said this was indicative of the Chinese strategy to focus on weak points in the network.

"China has also been using spear phishing, sending deceptive mass e-mail messages to lure DOD users into clicking on a malicious URL..."

Leo: They call that "spear phishing," huh?

Steve: Yeah, well, because instead of phishing, where you're just sort of broadcasting to anyone, a spear phishing exploit is, exactly, is targeted, and in this case at DOD users, DOD employees. So it's directly – and of course spear phishing means that they can also tune the content of the email to be more application specific. So it might be, you know, more prone to a DOD interest and look more authentic to people in the DOD.

It says, "China is also using more traditional hacking methods, such as Trojan horse viruses and worms, but in innovative ways.

"For example, a hacker will plant a virus as a distraction and then come in 'slow and low' to hide in a system while the monitors are distracted. Hackers will also use coordinated, multipronged attacks, the official added.

"Chinese hackers gained notoriety in the United States when a series of devastating intrusions, beginning in 2003, was traced to a team of researchers in Guangdong Province. The program, which DOD called Titan Rain, was first reported by Federal Computer Week in August 2005. Following that incident, DOD renamed the program and then classified the new name." So we don't know what it's called.

"That particular set of hackers is still active, the Netwarcom official said. He would not confirm whether the Titan Rain group was linked to the NWC attack or any other recent high-profile intrusions.

"Other senior military officials have spoken out recently on U.S. cyber strategy, saying the country urgently needs to develop new policies and procedures for fighting in the cyber domain.

"'Current U.S. cyber warfare strategy is dysfunctional,' said Gen. James Cartwright, commander of the Strategic Command (Stratcom), in a speech at the Air Warfare Symposium in Orlando, Florida, the week before. 'Offensive, defensive and reconnaissance efforts among U.S. cyber forces are incompatible and don't communicate with one another, resulting in a disjointed effort,' said Cartwright.

"Gen. Ronald Keys, commander of Air Combat Command, told reporters at the conference that current policies prevent the United States from pursuing cyberthreats based in foreign countries. Technology has outpaced policy in cyberspace, he said.

"'The United States should take more aggressive measures against foreign hackers and web sites that help others attack government systems,' Keys said. 'It may take a cyber version of the 2001 terrorist attack'" – meaning 9/11 – "'for the country to realize it must re-examine its approach to cyber warfare.'

"Netwarcom officials described their approach as an active defense, in which monitors build defenses around the perimeter of DOD systems, work to mitigate the effects of attacks and restore damaged parts of the network.

"Meanwhile, the consolidation of DOD's cyber resources is ongoing. Netwarcom works directly with the Joint Task Force for Global Network Operations, DOD's lead agency on network defense and operations, a component of Stratcom.

"Netwarcom, the Navy's lead cyber agency, is moving from monitoring the networks to full command-and-control capabilities. The Air Force announced in October 2006 that it will create a Cyber Command, based on the infrastructure of the 8th Air Force under Lt. Gen. Robert Elder, at Barksdale Air Force Base, Louisiana, to coordinate its cyber warfare efforts.

"In the end, the cyberthreat is revolutionary, officials said, because it has no battle lines, the intelligence is intangible, and attacks come without warning, leaving no time to prepare defenses. Education and training of computer users, not enforcement, are the most effective defense measures, officials said."

Leo: Well, we've kind of said that for a long time. That's what we do.

Steve: Isn't that, I mean, it demonstrates that the U.S. and certainly other nations on the globe are really taking this notion of the importance of our global network and the need to defend ourselves against, you know, deliberate attacks and intrusions into that network surface. And I thought it was really interesting, too, because we talked, it was last week or the week before, I don't remember which, about this idea of could good guys who had the best interests of the world and users and the network and so forth at heart, could they proactively do things to other people's machines that were good for them, for example, like since we had the IPs of worms on the Internet, and we even have them today, I mean, there are still instances of Blaster and Code Red and Nimda out on the 'Net, scanning around, still trying to infect machines. And if you put a fresh copy of Windows 2000 or XP on the network without its firewall in place and not behind a router, it'll get infected before long. That's now been proven and is well known. So that means that we all know the IPs of those machines. But the law protects us from fixing them, even though we could, since they were infectable by this problem, we could use the same problem to disinfect them, but doing so is illegal. And so similarly it's clear that in this report the military is saying that U.S. policy and law prevent them from doing to others what apparently is being done to us effectively.

Leo: It's unfortunate, after many years of being lied to by our government, I'm not sure I completely trust what they're saying. I'm trying to think of what ulterior motives they might have to this. And I'd hate to see them move towards locking down what we can do on the Internet, using this as an excuse for it. But I think that it's probably pretty clear that this is going on. Isn't it?

Steve: Yeah, I think so. And in fact, one thing that I find really interesting is that it seems that they're having such a problem in protecting themselves. Now, there was a reference to an Intranet, meaning that these systems that were vulnerable were apparently directly on the Internet. And so you could imagine, I mean, you know, DOD has humans, has people just like any others. And they've got their PC at home where they surf the 'Net and they click on links and they've got email. And the problem is, the experience is so much the same when they're on the Internet at work that they probably bring some of their casual habits that developed in non, you know, non-information, non-intelligence-critical environments, with them, and may without thinking click on a link in email. So to me it's really interesting that, with this much at stake, with national secrets, and the idea that somebody could, obviously, as we know, you click on a link, and your browser goes somewhere, you've got scripting active, there's, you know, a whole basketful of exploits that are currently known that allow even fully patched browsers to get compromised. So it's very much the case that I guess I'm surprised that these networks are exposed to the Internet, which we know is such a hostile place.

Leo: You would think, though, that if anybody could block and lock down their systems, it would be the Department of Defense.

Steve: Well, I have an interesting story that I've never told. It dates back about five years ago. A hacker contacted me, a white hat hacker contacted me, saying that he had gained access into Microsoft's internal networks. And I said, okay, I don't want to talk to you about this. I mean, I said, I don't want anything to do with this. Go away. And he said, well, I really think this deserves some attention. And I said, go tell Microsoft, you know, tell them how you're doing this if your interest is really to, like, help them do things better. And I said, look, you know. And he wanted to, like, send me some proof. And I said, no, you're not sending me anything. And he said, well, how can I bring this to public attention? And I said, well, if your interest is in embarrassing Microsoft, then you want to talk to some computer reporter, not me. I said, I am not going there.

So actually I did have a guy that I knew that I referred him to, that is a very active reporter in the computer industry who did receive, based on all of his, you know, reporter confidentiality agreements and things, he received some documents that proved to him that this guy really had penetrated Microsoft's network. And again, he urged the guy, I urged the guy, just tell Microsoft. Get a story written if that's what turns you on, but tell Microsoft.

But the point of this is, what he explained was that he had gotten in through some satellite network in a foreign country, I mean, a Microsoft remote sales or support office or something, got essentially onto a computer that wasn't as secure as it should have been. I think it was back in the Windows 2000 days, so it was a Windows 2K box that had some vulnerabilities. He was able to get into it. Once he was there, he was on a network, and so he established a presence on that machine. Then he was able to, within Microsoft's network – and this was arguably, and as I recall, I mean, this is a long time ago – he was able to go from, sort of leapfrog from an insecure Intranet to a much higher security Intranet by finding a machine that had dual network adapters. So somewhere there was somewhere, maybe at Redmond or who knows where, there was a machine that was straddling both networks. It was on the less secure Intranet and also had a presence on...

Leo: So it was a gateway.

Steve: Well, exactly. And so whoever it was running that machine, they needed simultaneous connection to both networks. And there was no hard division separating these two Intranets. So he was able to get himself onto, from a satellite machine, onto basically a more important machine that had two networks, and then essentially hop into the much stronger network through that means, setting up a relay point of his own at that machine. So I guess the point is that even a network architecture designed to be secure, where you really, really have spent time shoring this thing up and preventing anyone from getting in, if it's a sufficiently complex and sophisticated set of connectivities, there can be little loopholes that are not obvious, and that somebody determined really just sort of by exerting pressure from the outside, they can find a leak if they sit there and exert sufficient pressure.

Leo: Does this mean that the hackers will always win because there's just more of them, and they're more willing to work at this than anybody else is willing to defend? I mean, if the Department of Defense can't secure it, if Microsoft can't secure it, well, we don't have any hope.

Steve: Well, it's certainly the case that there are systems within the DOD that are off the Internet. I mean, we've all seen in sort of sci-fi movies where you go into a room that's just got a computer sitting there, and it's a super high-security machine. Well, you know there's no way that you can go www.google.com and, you know, you are not on the Internet on that machine. So you have to have a completely separate network with, like, no connectivity across. And certainly that's the case. But what happens is, people do want convenience. And it's always that case of, like, well, you know, I'll be really careful. I need to be able to get on the Internet, but I also need to have access to the internal DOD documents. So that's a point of vulnerability. And I think you could argue that with networks being so sophisticated, so complex with their interconnectivity becoming richer and richer, that there are ways to worm around inside.

Leo: Amazing. Well, let's hope that people are listening to this, and the Chinese aren't. And if you're in China, we're glad you're listening. And please don't hack us. Please, we beg of you.

Steve: Well, yes. And I'm a little skeptical of these guys saying, oh, this is supported by the Chinese government, you know, because of the nature of the attacks. We know that teenagers are running botnets of tens of thousands of bots and are able to administer huge attacks anywhere they want to, you know, bandwidth floods, and they're being used for spam emails and things. And if it weren't known that these were 13 year olds who were running these networks, we might think, oh, this must be some major government operation. It's like, no. It turns out that, you know, people are curious. And certainly in the case that I was talking about, this white hat hacker guy who, you know, I remember very little about him now, but he was just, you know, he was curious, and he was just poking around and seeing what he could do, you know. And it's illegal, and we want to make sure we stress that. All of this is illegal. But it's very possible to me that there are just non-government-backed people certainly all over the world who are poking at other countries' networks. I wouldn't be at all surprised if we're doing the same.

Leo: And I could provide you with evidence of that. If I look at my logs, and I bet if you look at your logs, I get every day hundreds and hundreds of attempts to find backdoors into my system, attempts to log-on via telnet and SSH. And almost all of them come from

Chinese IP addresses. I don't think the government's trying to break into TWiT.tv. And they're usually universities in China. I think there are a lot of kids there who, you know, for whatever reason, they like to – they're hacking, and they're trying to find a backdoor into my system. I can guarantee you that TWiT.tv is not a backdoor into the Department of Defense. Maybe they know something I don't know, but it's just, I mean, it's gone on for as long as I've had a web server. And they try to hack every service – SMTP, IMAP, you know. They hack services that I don't have. I'm sure they're automated. They're just trying every – and it's brute-force log-in attempts.

Steve: Well, and, you know, site defacing happens all the time. I have to think, too, that the way, based on domestic U.S. politics, there is some tendency for these guys to maybe overinflate the threat because they want bigger budgets.

Leo: It's not like they would ever do that, of course. It's not like that would ever happen.

Steve: Yes. Which is not to say these things are not possible.

Leo: That's the problem, it's hard to assess because – it's hard to assess. I guess that was my point. And that's why it's too bad we don't trust our government a little bit more.

Steve: Well, and, you know, you could also argue that the U.S. was caught off guard on the morning of 9/11, and that since we've done things to make ourselves safer. This guy makes the point that it may take something like that in order to get the government to say, oh, maybe you guys do need some more money for more fancy security and networks and so forth.

Leo: There was, right after 9/11, of course, there was a cyber security czar, and there was a lot of attention paid to this. I don't know if that activity's waned, or if it's still part of Homeland Security. I imagine it still is.

Steve: I'm sure there's a title on a door somewhere. But the question is...

Leo: Who's inside.

Steve: ...how much money are they being given. It's all a function, I mean, it all comes down to money, what you're able to afford. And we've heard stories, for example, about how the FBI's network is just horribly antiquated. I mean, just, you know, just almost punch cards. And it's like, okay, well, maybe you can get rid of those old copies of WordStar and WordPerfect one of these days.

Leo: And soon as J. Edgar Hoover – oh, wait a minute, never mind. Folks, this podcast is sponsored by Iwanttobeanerd.com. That's the folks at Nerds On Site. They are a great group. They're growing, too. And they need more nerds to service their customers. Looking for folks with competencies and skills in all areas, from PC and Mac experts to specialties like Cisco and Oracle. You name it, they need it: fix-it technicians, website designers, programmers, project managers, sales folks, trainers, security experts, antivirus gurus and more. They especially love those nerds who troubleshoot, tear apart, and rebuild their own

systems in their spare time. You know who you are. Nerds are independent contractors. You're in business for yourself. But not by yourself. And I think that's what I like so much about Nerds On Site. You can focus on your passion, but they handle the burdens of running the business. Now in seven countries – Canada, U.S., Mexico, England, Australia, South Africa, and even Bolivia. And if you want to know more, go to Iwanttobeanerd.com and register for a nerds-only meeting in your area today. Good people. Our people. Iwanttobeanerd.com. That's Nerds On Site. We thank them so much for their support for Security Now!. They love you, Steve. They see one of their own.

Steve: They're good guys. It's funny, too, because you mentioned the site that had a video of me. And I was curious, last week I went there thinking, oh, you know, what's this going to be?

Leo: What did they tape, yeah.

Steve: And what was cool, it was me telling them the story that I had told to our Security Now! listeners before about this guy who was fired because SpinRite saved this cute old lady's drive. And so, you know, it must have been before I told it on Security Now! that I was up in...

Leo: I think it was because you were in Toronto, yeah.

Steve: ...Toronto. And I told these guys the story. And so that was a little short video, I don't know, it was like five or six minutes of me, you know, waving my hands around in the air as I am apt to do, telling them this story of – and, you know, it's funny, too, because the first thing they said when I told them that the younger, junior, good repair guy was terminated because he was willing to take, like, double the time and to run SpinRite and recover the data, rather than just reformatting this poor old lady's machine. And the first thing these guys, the nerds said was, who is he? We want to hire him. We want him to be one of our nerds. So, you know, the kind of guys they're looking for. So it was a fun story, it was a perfect story for their site.

Leo: Nerds On Site. Iwanttobeanerd.com. We thank you all for being here. And of course, if you want 16KB versions of this show, we make them available on Steve's site, GRC.com. We also offer transcripts there of the show so you can read along with Steve. And there'll be links there to the original document, the Cyber Warfare document that started this whole discussion off. That's GRC.com. That's also where you'll find all of Steve's free security products, including ShieldsUP and the new SecurAble and, of course, SpinRite. Got trouble with your hard drive, SpinRite is the answer. GRC.com.

We'll be back next week and talk more about security. Okay, Steve?