GhostNet

Description: Steve and Leo begin by discussing the week's security news. Then Steve carefully and completely describes the construction and operation of a worldwide covert cyberspace intelligence gathering network, operating in 103 countries, that was named "GhostNet" by its Canadian discoverers.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-191.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-191-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 191 for April 9, 2009: GhostNet. This show is brought to you by listeners like you and your contributions. We couldn't do it without you. Thanks so much.

It's time for Security Now!, the show that talks all about your security, your privacy, how to protect yourself online. And Steve Gibson's our man. If Steve can't do it, no one can. He's from GRC.com, the creator of SpinRite, the world's best hard drive maintenance and recovery utility; also the discoverer of spyware, the guy who coined the term "spyware," and a security advocate going way back. Hi, Steve.

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

Leo: How is everything going in...

Steve: Really good. I got distracted for a couple weeks and pulled away essentially from the work on the DNS benchmark that I hope to be, maybe in two weeks, telling our listeners about because it has ended up being very cool, and we've learned some things, interesting things about home routers and why you don't want them to get involved with your DNS, although by default they typically are now, more and more. And I did also, brought myself up to speed on today's topic, GhostNet, which is an interesting report that was generated by two research groups up in Canada. And it's got me thinking about

the whole botnet tracking deal, and I have half a mind to set up my own little Conficker honeypot, just I think it would be fun to watch Conficker run. Of course, you know, security firms all over the world have Conficker honeypots. And it's like, okay, well, it'd be fun to have a little first-hand information about that, too.

Leo: Conficker.

Steve: Yeah.

Leo: So you could set up your own Conficker receiving center?

Steve: Oh, easily. I'm sure that my attachment folder, my Eudora attachment folder...

Leo: It's full of Confickers, huh?

Steve: ...is full of Conficker. It's just - yeah. In fact, what I'll do is I think I'm going to put avast! back on the machine that I used for scanning my friend's laptop a couple weeks ago when hers got infected, and then just drag the whole - make a copy of my Eudora attachments folder over to that machine and then stand back while avast! says, oh, avast ye maties.

Leo: [Mock screaming] Run, run for your lives, run for the hills.

Steve: I'll find some, and then I'll just install XP on a honeypot machine, and not patch XP; open one of those attachments. That'll infect it. It'll jump onto the Conficker botnet. And then of course I'll have packet-sniffing going on, too. So I can watch it do things, which is...

Leo: Oh, ought to be very interesting, yeah.

Steve: Yeah.

Leo: Yeah. You're a brave, braver man than I, however.

Steve: Well, I've got a cable modem with two IPs from Cox. So I can give it its own IP. I'll put it behind its own router so I'm not looking at the cable modem traffic, but only the infected host traffic. And, I mean, I've done that before, back when I was tracking down the weenies that were attacking me.

Leo: Right.

Steve: And basically it was - I have a story, of course, that was very much like what we're going to be talking about this week. But these guys were - the ones that we're talking about this week are clearly politically motivated. Whereas before it was just, you know, the 13 year olds screwing around with botnets when botnets were in their infancy. Now, of course, botnets are a big, profitable enterprise.

Leo: We're going to talk about GhostNet, the spy - and, you know, there was a story in The Wall Street Journal, I don't know if you read this, I think it was yesterday, that there are also spy programs that are being found in our grid, in our national electric infrastructure. And of course that's exactly where, if you were going to do cyber warfare, the first thing you'd go to is the grid. And this is a fascinating story. So I'll read to you a little bit from that, too. And I think it's probably very similar to the GhostNet story. All right, let's talk about - do you want to do any errata from previous shows?

Steve: Oh, always have security news and a little bit of errata, or miscellanea. On sort of a separate, not quite really directly related topic, you probably saw yesterday, Leo, that the U.S. Justice Department came down with a very disturbing decision related to warrantless wiretapping?

Leo: You know, I saw the headline, and I didn't read it. What did they decide? Because this is a scary thing.

Steve: It's got the constitutional scholars very upset.

Leo: Oh, dear.

Steve: Apparently...

Leo: I had really hoped for better, frankly.

Steve: Yeah, we all had from Barack's administration. But one of them was explaining that no President has ever walked back any rights which were - that had been obtained by any previous presidents.

Leo: Of course not.

Steve: Which is another way of saying it only keeps getting worse.

Leo: Yeah, of course. Why would you give it back unless you had...

Steve: Exactly. Why, well, you know...

Leo: ...a lot of integrity or something...

Steve: Exactly.

Leo: ...crazy like that.

Steve: And, you know, he's been out of the country. So but apparently this - this looks like it's clearly coming from the administration. What the decision was that came down from Justice was that, relative to warrantless wiretapping suits, because several suits have been brought by people, for example, against AT&T, who was one of the participants in the warrantless wiretapping probes that was revealed during the Bush administration, a bunch of people sued them for this being unconstitutional. The Justice Department said that the government will be held harmless and that no action can be taken except in the instance of deliberate, voluntary disclosure of the information. Which, you know...

Leo: In other words, if they leak it, okay.

Steve: If they deliberately leak it. Not even if it leaks. If it's deliberately exposed, then that opens the government to consequences. But don't even think about it. You have no standing in the event that, even if you learn that you've been spied on, that's okay. And one of the constitutional scholars, I don't remember his exact phraseology, but I found it really interesting. He said it's not possible to have a right without having the ability to defend it, I think is sort of paraphrasing what he said, which I thought was interesting. It's like the point is that this has completely removed any defense. I mean, it's completely removed any action that someone can take when they've been wronged. Even when it's clear that they've been wronged against the law, then this supersedes that, and there's no action that can be taken.

Leo: They're claiming that government is, quote, "completely immune from litigation for illegal spying. The government can never be sued for surveillance that violates federal privacy statutes." Now, this is just their assertion. This is just a brief. It's not the law of the land. I hope the court goes, ah, excuse me.

Steve: Good.

Leo: Fourth Amendment. Because that is just appalling.

Steve: Well, it's like, okay, wait a minute. How did this happen? This is not what we were supposed to get. But, well, maybe we did. We'll see.

Leo: Well, I think you might have hit the nail on the head. Nobody's ever stepped back from a - that's why we've got to be eternally vigilant in restricting the power of

government because, once it gets it, it is...

Steve: Once it goes forward, yes.

Leo: And, you know, they're protect- I think what this does essentially is, the point is, they protect the previous administration, hoping that the next administration might protect them should they do anything like this.

Steve: Yeah, and you know, I have been, I mean, I don't want this...

Leo: It's collegial.

Steve: ...to get into politics. But I've been pleased that there isn't this let's go attack the prior eight years. I mean, it's like, Barack really seems to have it. Let's just move on and...

Leo: I think that's the proper thing. But this may be the case where moving on is not the right thing to do. Although maybe the feeling is this is the last thing we want to do is get in a myriad of court cases over NSA wiretaps and so forth, wireless wiretaps. Good article in this on the Electronic Frontier Foundation site, if you want to read more about this. They are very active, of course, in these kinds of things.

Steve: On an annoyingly related note, the U.K. passed on Monday their version of this EU edict, essentially, which has increased and formally ratified the data retention which is being done of all citizens in the U.K. and which is supposed to be adopted across the whole EU. They've added to the previous data retention guidelines the requirement for ISPs of all manner to record for a period of no less than 12 months the sender, recipient, date, and time of all email sent.

Leo: Oh, boy.

Steve: So there was - and the caller and recipient of any Internet telephone calls. There was already legislation in place that required the location and details of regular landlines and cell phone calls to be retained, and even for cell locations to be recorded when they were knowable. And so what's been added is now any outgoing email, not the body of the email itself because that's just way too much to record, but the sender, recipient, date, and time of all email sent, will now be recorded, retained by the ISP for up to 12 months. I mean for no less than 12 months.

Sweden is apparently just ignoring the whole thing outright, just saying, uh, no, we're not doing that. And Germany is challenging it in the courts. But the U.K. signed into law on Monday an adoption of this. And so all U.K.-based ISPs, apparently they're complaining about it. They're complaining about the cost. And the U.K. said, well, we will pay for the cost. We will underwrite the cost of doing this. We need this for the sake of the security. There's an Isabella Sankey who's a policy director at Liberty said that the

directive formalized what had already been taking place under voluntary arrangements for years. But she said the problem is that this regime allows not just police to access this information, but hundreds of other public bodies. And, I mean, that's always the concern here is that you end up with this big database. And then people go, oh, you know, that would be useful for something else, as well. You know, the repurposing of data is really a concern.

Leo: Yeah. Rightly so.

Steve: In other news, and this really relates to where we're about to go with the story of GhostNet, there is a newly discovered, zero-day, unpatched, PowerPoint vulnerability which is now being used in targeted exploits. There have been PowerPoint little PPT files found in email, so-called "spear fishing," where they're sent to specific email accounts, specific individuals, targeting them specifically. This hasn't been yet found in wide-ranging spam because if anyone finds an unknown - any bad guy finds an unknown, unpatched exploit, they recognize that they only have some length of time to use it before it gets found, and then we start the patching and the AV pattern updating cycle. So it makes sense that, if a new vulnerability is found, it's going to be kept under wraps, and as much use of it will be made prior to using it widely. You're not going to want to spam the world with it until you can no longer get maximum value from it by doing targeted attacking.

And so right now we're at the target attacking phase. Microsoft has a page on their site acknowledging this. They've seen it. They know it's happening. Of course here we are with the second Tuesday of April is the next Tuesday for our recording. So by the time we hear from you again, or by the time our listeners hear from us again, we'll know whether Microsoft made this into their April patch round. At this point we don't know, and there is no patch for it, no fix for it. But Microsoft has acknowledged it. So it's just one more in a continuing, literally weekly flow of new vulnerabilities being found in the software that most of us are using.

Leo: That's amazing. You know, you'd think that it'd slow down after a while.

Steve: Gosh. Well, if the new software kept being...

Leo: Or we'd find them all or something. But I guess it's like weeding. Yeah, exactly right, it's like weeds. They just - new ones sprout up all the time.

Steve: And I also wanted to ask you, because I've seen a whole bunch of positive feedback about my recommendation last week of Tree Style Tabs, are you still using...

Leo: Been using it. Love it.

Steve: Yes.

Leo: Not only that, Sarah Lane came in and said, "Where's my tabs?" And I said, "Oh, they're on the side." And she said, "Oh, I like that." So, yes, it's great. Good choice. This is a Firefox extension.

Steve: Yup. So everybody using Firefox on any platform can use it. It seems to have fewer features over on the Mac platform. I like some of the things I can do under Firefox and Windows with it. And one person posting in our newsgroup said something I didn't realize. If you've got a hierarchy of tabs because you've opened some links underneath an existing page, just dragging the parent tab to another Firefox window brings all the kids.

Leo: Oh, I like that.

Steve: Yeah. So you're able to, like...

Leo: That's really handy.

Steve: ...create a new window that has a whole subset of the tabs that you had opened, the hierarchy underneath a given tab just by grabbing the parent. Which is...

Leo: Very clever.

Steve: Very cool.

Leo: Very, very clever, yeah.

Steve: Yeah. So I just wanted to reiterate for people who haven't made the jump or who weren't curious, maybe, you know, we're getting great positive feedback from that recommendation. You might want to check it out.

Leo: What's the actual name of the add-on? Is it Firefox Tabs?

Steve: I think it's called Free Style Tab, three words. I'm sorry, Tree. Tree Style Tab.

Leo: Tree Style Tab, that's right. And the version I'm using on the Mac is 0.7.2. But I would imagine it's the same, I mean, it gives you a lot of preferences. You know, actually I haven't really dug into this much.

Steve: I know. It's, like, overwhelming. I thought, okay, wait a minute, I'm just - I'm going to start using it first because I don't know if I want to change any of these settings yet. I want to use it the way the author has defaulted it, and then maybe after I'm

familiar with it I'll go, oh, look, I can push this button over here, and it'll do something a little better for me.

Leo: It's even got different views. Different appearances and...

Steve: Yeah.

Leo: Wow. Wow. I didn't - yeah, you're right. I didn't - wow. This is quite more - I had never looked at the preferences. This is quite elaborate.

Steve: It's like, okay, wait a minute.

Leo: Oh, I don't even know what all that stuff does. Holy cow.

Steve: So this was posted by Anthony in Australia. And I don't recall, I haven't recorded whether it came in through email or the newsgroup or what. But he sent me a note, he said, "SpinRite on par with Craig Venter's brilliance."

Leo: Now, you know who Craig Venter is.

Steve: Well, I didn't until I got down to the end of his message.

Leo: We interviewed him on The Screensavers.

Steve: Oh, no kidding.

Leo: Yeah, one of the most important people of our generation, I would say.

Steve: Well, I don't think SpinRite's quite on a par with that.

Leo: Go ahead. I mean, it's quite - it puts you right up there, I'll tell you.

Steve: Oh, it was in his blog. It was a blog posting...

Leo: Oh, how neat. Oh, how neat.

Steve: ...he made on February 20th. And he said - it had tags: SpinRite, Steve Gibson, and GRC.com. And then he blogged, he said, "Some feedback I just sent to Steve

Gibson, the creator of SpinRite (v6) at GRC.com." He said, "Hi, Steve. I'm a long-time Security Now! listener and SpinRite user. And today was one of those blue moon days where SpinRite saved our bacon. No dramatic special ops story here." And he has a little smiley face. "But satisfaction and gratitude abound, nonetheless. And perhaps a new point of view on why SpinRite is so awesome." It's interesting because the other reason I wanted to read this, this is the long posting that I skipped last week because we already had a super-long podcast.

Leo: We had a long - right, right.

Steve: But he brings up something that has been asked before, but we've never talked about. Anyway, I'll get to that in a second. So he says, "Our FoxPro developer's old Dell laptop, which had been trucking along fine for years, suddenly wouldn't boot this morning, BSODing during every boot attempt. And, as usual, Safe Mode was no help. He's usually a stickler for doing frequent backups. But when I asked how long since the last backup, I got back only an embarrassed, sheepish smile. Oh, boy.

"Recognizing immediately that this was probably SpinRite's cue to enter from stage left, I put it to work, and in about an hour it had completed. Although there was no record of any bad sectors found or corrected, I did notice it churning away for several minutes on a few spots, and I suspected I was on the right track. (No pun intended)," he wrote. "Sure enough, after SpinRite, the laptop booted right up. And so far all looked to be intact. A backup has now been performed, and the impetus to replace the laptop very soon has been renewed. Just another" - and he says, "Just another day at the office for SpinRite, but a significant potential loss averted for us. Thank you so much for such a legendary product. I promise to buy another couple of licenses to reach my consultant's license status ASAP."

And he said, "By the way, while doing a bit of research into SMART a while back" - that's the Self-Monitoring Analysis and Reporting Technology, SMART, acronym that's built into all contemporary hard drives - "I stumbled across a hard drive data recovery expert's site which had a page recommending data recovery and utility software. At first I was surprised not to see SpinRite at all, let alone at the top of the list where it should be. Until I saw a note where he explains that he (paraphrasing) 'disqualifies SpinRite because it doesn't make a copy of all the readily accessible data before attempting restorative measures, and thus puts more data at further risk.'"

He said, "I understand the logic behind this argument, and I agree that in rare circumstances a drive may degrade to such an extent or have physical damage to the heads, for example, and not be diagnosed until it's hanging by the proverbial thread, and thence SpinRite's thrashing may snap that last thread. But you know what? Having used SpinRite myself since the early '90s, and hearing all your testimonials on Security Now! every week for three years, and hear you explain how it and hard drives work, I've come to realize that most hard drives' magnetic media failures don't fall into that severe category, and that SpinRite's approach offers far more bang for my buck than data recovery specialist services, which are what this guy was recommending.

"Whilst he's probably just taking a very conservative approach, understandable in that industry, someone more cynical than myself might suggest this guy's wowser attitude is not in his customers' best financial interests. Even more cynical people might wonder if some of these data recovery specialists secretly use SpinRite themselves to recover data from customers' drives and charge traditional (read exorbitant) data recovery prices for it.

"I'm reminded of the race to decode the human genome in the '90s, with the purists using a stubborn, narrow-minded, linear sequencing technique that was threatening to take forever, and Craig Venter's maverick scatter gun recombination approach, which won the race. I see your unique and novel approach to tackling magnetic media failure in exactly the same light - simply brilliant."

Leo: Well, there you go.

Steve: That was Anthony's note and posting.

Leo: I'm with him on that one. I mean, saving the data seems to me unnecessary.

Steve: Well...

Leo: I mean, you could do it if, I mean, often when I tell people to do a drive recovery, I say work on a copy of the drive, if you're really worried about the data. But that...

Steve: Right.

Leo: SpinRite wouldn't help in that case. You'd make a copy, then have to work on the original drive, wouldn't you.

Steve: I guess I'm of two minds. The way SpinRite works, that is, doing an in-place recovery, does have, I mean, there is the possibility that, if the drive is absolutely determined to die, then nothing any software can do can prevent that from happening. And if it's going to happen at some point, then when you're using it is probably when it's going to happen. SpinRite's in-place recovery probably owes more to its history than anything else. You know, I wrote it first back in the late '80s when a 10MB hard drive was a couple thousand dollars. People didn't have extra hard drives. You were glad to have one. I mean, if you had one, your friends who were still shuttling floppy disks in and out of their floppy drives, they were envious of you. So there wasn't this whole notion of, oh, just get another drive and copy the data over to it.

So doing an in-place recovery really made the most sense. And the fact is, while I understand the theoretical point that that guy, that data recovery expert was making, I have now 20-plus years of experience with SpinRite's actual use. And we see virtually no instances of, I mean, yeah, maybe anecdotally it's happened a few times where, while SpinRite was working on the drive, it gave up.

Leo: Yeah. I've never seen that.

Steve: It almost never does. And typically what's happening is some sectors are getting in trouble, you just use SpinRite to bring them back, and then you're okay. And had you

used SpinRite the week before, then the problem would have never happened in the first place. So drives are dense enough that they're always sort of on the edge, but using error correction technology on the fly to keep them looking fine. SpinRite isn't fooled by that, and so it's able to go in and fix problems before they manifest and, fortunately, to fix them even after they have manifested. But in all cases, these are not drives that are about to completely go belly up. Fortunately that happens very rarely. It's mostly that people's data becomes endangered long before that actually happens.

Leo: Right.

Steve: And of course, as soon as they can't boot, they know something's wrong. But that's, like, long before the drive is completely toast. And so SpinRite can typically bring it back to life.

Leo: All right. Let's talk about ghosts.

Steve: Okay.

Leo: [Moaning]

Steve: So this is a really interesting story with lots of information and details that I think our listeners are going to like. And I learned something really interesting, too, about the evolution of command and control in these networks that I think everyone will find interesting.

The story begins about nine months ago, when the representative of the Dalai Lama in exile asked an affiliated group - there's something called the SecDev group in Canada and the Citizen Lab, which is at the Munk Center for International Studies at the University of Toronto. And these two groups work together on, and have in the past, on issues of cyber stalking, cyber terrorism, cyber attacks, that whole sort of area. And they have a political orientation. I mean, so the international studies side.

And so about six years before that, in 2002, the group had been involved with the Dalai Lama, with some sort of malware. The Dalai Lama's organization was being targeted through direct malware attempts to infect their network. And so these guys became involved. So they were asked to, I guess through some sort - there was, like, a meeting where they were just sort of talking casually about, well, maybe we need to do some sort of education to inform the people who work in our offices and on our network what they need to be doing to be safe.

And as a consequence of the conversation, one thing sort of led to another, and the person who was the executive with the Dalai Lama's organization said, well, you know, why don't you just sort of take a look at our offices, meet a couple of our people, maybe check out our network. I think in the process of having this conversation some concerns had been raised. So they took a look at a couple machines, and sure enough, they discovered some malware that they were previously unaware of.

They put Wireshark - which is the open source, publicly available sniffer, it's the one I

use myself, a very nice program - they put it on the machine and did some traffic captures of traffic that was transacting with that machine. That allowed them to see a communication that was being made autonomously by this machine to an IP that happened to be on the island of Hainan in the People's Republic of China. They tracked down the IP, looked at reverse DNS, checked the listings. It was just a commercial Internet service provider, a standard Internet provider IP. And what was interesting was that they then checked - they then went to that machine, not physically, but over the 'Net. And they discovered that the command-and-control system that was at the receiving end of this client-initiated communication was - it had an open access web interface. So using just a regular web browser, they connected to this server, certainly taking all kinds of precautions themselves, I'm sure, and began the process of figuring what was going on.

What they - in looking at this machine, which this first client machine, which had been infected, they found some - they found this malware content in a number of documents which had been attached to email. So this is exactly the kind of infection vector we've talked about often, and which I was just talking about relative to PowerPoint slides and this currently unknown or, well, now known. But it was discovered the wild, so it was a zero-day exploit because it was being exploited before it was known. In this case it was an old problem in Microsoft Word from 2006 that was still two years later being exploited because this particular machine had not been updated in that length of time.

Leo: Oh, boy.

Steve: So these non-updated machines create this window of opportunity. So by logging in to this command-and-control web interface with a - they discovered that this was a software system called Ghost Rat, for Remote Access Trojan. And literally Googling "Ghost Rat" and clicking on, like, four links, I had the source code for it yesterday. It's an open...

Leo: Wow, that was easy.

Steve: It's an open source...

Leo: Open source, great.

Steve: I have v3.6 beta.

Leo: Oh, man.

Steve: Was the one that I...

Leo: This shows you, I mean, these are professional programmers writing this at this point.

Steve: Actually, it shows signs of not being...

Leo: Oh, interesting.

Steve: ...that professional. First, well, for all kinds of reasons that we're going to talk about.

Leo: Oh, interesting.

Steve: I want to sort of run through the timeline, and then you and I are going to talk about a lot of what this all means. But in looking through the source, I saw first of all comments in Chinese, which my own Visual Studio didn't translate for me. But what I saw was, like, lots of sort of canned chunks of things, like sample code that had been pulled from various Microsoft tools, just sort of glued together by a little bit of custom code. But this thing is, you know, way bigger than it needs to be. And it's just sort of pulled together to do the job. It's been around for some time. And it's funny because in the forum where I found this there was a bunch of people who were having trouble with error messages. And well, you know, I didn't - I wasn't sure whether I had to install the DDK or not, and I'm not really quite sure how to get rid of these error messages. Can someone give me a hand? And so this is - and this forum where I found it was a trojan horse development forum with, I mean, this is just all now out in the open. Just, you know, a couple clicks, you Google "Ghost Rat," and you'll find the source code for it.

So interestingly, now, back in the day, as they say now, back when I was first involved in this myself, in backtracking attacks that were being made against GRC, you'll remember that - and we've talked about this a number of times, that the botnet then was based on IRC chat. So when you got yourself infected, if you were unlucky enough to do so, the client that was the infection would make an outgoing connection to an IRC chat server somewhere. IRC chat was convenient for the bad guys to use because this IRC chat network is itself a network of interconnected servers that will relay chat messages among them. So it's not necessary for the bad guys, the bot masters, to be logging into that same server. In doing so, they would be vulnerable to being caught because that server, I mean, it's easy to find a server. You just look at the IP that the IRC connection is being made to. Now you know where this bot is going for command-and-control coordination. Then you look at all the incoming connections to that channel of the IRC server, and it's easy to track down the IP of whoever is issuing the commands.

So instead, by using IRC, you've got sort of a federation of affiliated servers and the bad guys can enter the channel on a completely different, unrelated server, which will then forward their commands throughout the network until it finds the channel on the server where it's destined. So it makes backtracking them much more difficult.

So that was the technology, what, six, seven, eight years ago. Today things are different. What I found most interesting is that all of the protocol being used for command and control is just HTTP.

Leo: Really.

Steve: Yes. The...

Leo: That makes sense, though, because that's least likely to get filtered; right?

Steve: Well, get a load of this. It's even disguised. That is, the client makes an outbound web connection to this web server, which is the command-and-control web server. It does it to a PHP page, asking for a PHP page or in some cases running a CGI script, which is very common for any kind of automated pages. So it's just a standard port 80 HTTP connection. The commands are sent back encoded in JPEG images. So even if you were watching the traffic, you'd just see web activity with an image being retrieved in response to a PHP query, which happens all the time every day. I mean, that's the way the web works now, more often that not, in fact.

But the commands, instead of just being out in plaintext, they're bound into image files, which are being retrieved by the client. So unless you really knew that a given IP was malicious, you'd have no reason to suspect it from even looking at the packet traffic going back and forth. And as you said, Leo, it's also not going to be filtered. You could imagine that all kinds of people are now blocking IRC from crossing their firewalls and routers. But you can't block regular web traffic without incurring all kinds of problems. So, I mean, even if you proxy it, you could also have a proxy which is accepting the request, forwarding the request, accepting the returning image, and returning that to the browser. So even proxies in line would allow this to pass through. So that represents a real evolution in the way these networks are being organized.

But what's really interesting, though, is when these guys logged into the first of these control servers - they refer to control servers and command servers as separate. the command servers are the source of updates and images and documents. So essentially the client contacts the control server. The control server returns instructions for how to contact the command server, which the client then autonomously does. It receives commands from this second command server and then returns a status back to the control server once the command has been executed. So it's a fairly sophisticated relaying system designed to keep one side from knowing what the other is doing, essentially, unless you're really monitoring all the traffic at the common point.

One of the interesting things that they discovered is that the web interface lists all the machines of which it is aware, that is, all the clients, the infected clients which have contacted it, the date of first contact, the date of most recent contact, and includes links that you can click on for sending commands to these things. So it's got a complete, mature, point-and-click user interface and a database which is maintaining essentially a history of the malware's contact with this control server. So naturally, I mean, this thing lists all the IPs of the machines that have contacted it. So the researchers were able to say, oh, we just found the mother lode here.

They of course did reverse DNS lookups on all the IPs. They did whois queries to find out who the registrars were. They ended up, it turns out, having access through their connections to a number - many other machines that were either in networks affiliated with the Dalai Lama or in other Tibetan organizations, non-government organizations. They were able to visit those machines. They found in some cases multiple instances of this Ghost Rat software. That's why this whole thing was called GhostNet, by the way, if that wasn't clear. They found in some cases multiple infections that were contacting multiple control servers. That allowed them to then expand their search to and access other control servers, which they did. They ended up finding four control servers, all located on the same island in the People's Republic of China, and six command servers that were not otherwise affiliated. However, all of the domain name registrations pointed back to the same single individual. So this network...

Leo: Oh, that's interesting.

Steve: And thanks to this database that each of these control servers was maintaining, they could see that this whole network went back several years, back to the date of that original infection, or that original infection vector, back in '06. So this whole network had been in place for some time. Some machines didn't stay infected very long. That is, they could see from the logs that the date from the first contact to the last contact was only maybe 10, 20, 30 days. Some machines were infected for several years. They got themselves infected, and that infection just sat there for several years, contacting the control server periodically to see whether there was anything that the control server wanted them to do.

They were able, of course, now that they knew what the software was, and they could look at the command interface, they were able to see that these things could basically take an inventory of the client, the infected client machine; could exfiltrate, using their term, any and all documents on the infected machine; could turn on a microphone, if present, and stream audio out of that client to a given target; and the same with the webcam - turn on the webcam and stream video in real-time out of there. So, you know, basically - oh, and execute any arbitrary command on the machine that they wanted to as a remote access software.

So fundamentally they had complete ownership of these machines. And in some cases they saw evidence of the commander who was running these control servers watching an email dialogue between affiliated entities and inserting a spoofed email towards a not-yet-infected endpoint. And having been able to see the conversation, the bot master or the net master was able to create an email which flowed with the conversation and contained a malicious document which was opened by the recipient, for whom this email made total sense. They were expecting something like this, or this wasn't out of the ordinary. They opened it, got infected, and that new client then contacted the control server. So you could see how this network was being perpetuated and being maintained.

In one instance during this investigation, somebody who had worked in some capacity with the Dalai Lama was attempting to go back to visit her family and was stopped at the border, held for two months, interrogated. And when she claimed that she was not involved in politics at all, there was nothing political going on, she was just doing studies, they showed her, the authorities showed her a complete transcript of her private conversations which she had had previously. So this was information that the intelligence agencies of China did have in their possession.

Leo: Wow. So I was initially skeptical, I think as were you, that it would be China because of course any good hacker covers his tracks. But this sounds like, all told, given the evidence including the Chinese comments, the location of the servers, the registry, that it's pretty clear it's coming out of China. But what's interesting is it doesn't sound like it's very well done. You'd think the Chinese government wouldn't be going to forums to get their code.

Steve: Very good point. And so there are a number of questions which are raised. First of all, we have the fundamental problem of attribution. The attribution problem is a classic problem that law enforcement has because, yes, what do we know? I mean, what is provable? And that's the problem, of course, is the threshold of provability is much higher than what is guessable. So we know that there are four servers, all located in an

island. Actually it's the same island as where the Chinese intelligence organization is. But they're not Chinese intelligence organization IPs. They're just random ISP IPs. We don't know that - we know nothing about who is connecting to those servers because these investigators had no physical access to those actual four control servers. You'd have to have physical access to them to then watch all the traffic coming out of them in order to see who was connecting and accessing that web interface and taking command of it. So the Chinese government, that obviously and continually denies any involvement, may in fact not be involved. I mean, we don't have any evidence to say otherwise.

Leo: I would think, I mean, if our government were doing it they'd have these hack- good programmers at the NSA writing stealthy code that isn't - it's not out on forums anywhere.

Steve: Well, Leo, you know, as I've told you, I've declined some of those requests.

Leo: Right, right. You can be sure that not everyone has declined those requests.

Steve: And my code would not work this way, and no one would find it, and I'd be using packets no one had seen before.

Leo: And given the resources and the size of China and, frankly, the number of great programmers China has, I find this hard to believe that this is a government effort.

Steve: Well, and the fact that the web interface wasn't password-protected. All you had to do was know what IP port to browse to, and like what directory structure apparently - there was some reference made to needing to guess the location of the page, the web page that contained the interface. Yet these guys with no specific knowledge were able to guess in four instances and find the web interfaces on four different machines.

Leo: That's absurd, yeah.

Steve: Which are wide open and unprotected. So that's nuts, too. Now, on the other hand you could also say, oh, aren't the Chinese government clever to make it look so amateurish, that is, to use v3.6 beta of the Ghost Rat because we're going to draw all the same conclusions. I mean, it does give them plausible deniability. If you have something really high tech and robust, that is, nothing like it exists out on the public domain, then if, or we might say when, it's inevitably discovered, because all these things ultimately are, it's like, ooh, now it's much harder to say that's not, you know, high-end NSA or the equivalent of Chinese intelligence activities. Here, this looks like random people. Well, and in fact my personal take is that it's somebody, probably a nonprofessional, who's using public domain tools, who's focused, who's got strong political incentive, who's probably feeding documents that are uncovered to authorities, but that the authorities are not themselves doing this. It's just somebody who, through nationalistic pride or political beliefs or whatever, is doing it. I mean, again, we have...

Leo: Probably with the tacit approval of the Chinese government. I mean, this is certainly...

Steve: It's useful information.

Leo: ...consonant with their aims. Yeah, it's useful information. But it seems a little hard to believe that their government is doing this.

Steve: And so the other thing that we have to come away from with this, I mean, if you Google Ghost Rat and you literally, in four clicks, you own the source code - oh, and Windows binaries are available, if you don't want to assemble this or compile it yourself. You know, what does it take to perform an attack? It takes having a PC and being a little involved in the underground so that you're in the communication flow of, oh, look, here's servers that are compromisable. Here's, I mean, it's not even necessary to be on the leading edge because, as we've seen, there are computers that are exposed for years to known vulnerabilities. So it's not like you've got to be someone using, like, this PowerPoint exploit that we just talked about. Clearly you can be - the way Conficker is working, you can be using something that was fixed in October of last year and still a huge number of machines are available.

You know, to me it looks like this particular trojan is being used specifically for politically oriented work. In fact, what they found, what these researchers found, they found the four control servers, six command servers. By processing all of their logs, they ended up tracking down 1,295 discrete machines. And these are - the machines all have IDs. So even if they're on dynamic IPs, the logging technology recognizes the machine is connecting from a different IP. So this is all - the IPs have been disambiguated, or the machines have, rather, independent of whatever IPs they happen to have from time to time. So there's 1,295 individual infected machines in 103 countries.

Leo: Wow.

Steve: 30 percent of those are what this group considered high-value targets. You're going to end up picking up some debris from just random machines that get infected. But, for example, the machines that they were able to find and track down using reverse DNS on the IPs, and in many cases the machine names, the names of the machines are also posted in the log on the control servers. They confirmed that they found machines that were infected in the ministries of foreign affairs of Iran, Bangladesh, Latvia, Indonesia, the Philippines, Brunei, Barbados, and Bhutan; and the embassies of India, South Korea, Indonesia, Romania, Cypress, Malta, Thailand, Taiwan, Portugal, Germany, and Pakistan. They found machines in the Association of Southeast Asian Nations Secretariat, the South Asian Association for Regional Cooperation, the Asian Development Bank, a number of news organizations, an unclassified computer at NATO headquarters, and - I got a little kick out of this - and one machine in Deloitte & Touche in New York.

Leo: Why Deloitte & Touche? That seems like the outlier there, doesn't it.

Steve: Yeah. It's just - and there were a bunch of others that weren't even worth naming.

Leo: But these are for sure all in the same net. I mean, they're not...

Steve: They're absolute - yes. They're known in the same net. Those machines were repeatedly contacting these control servers. And these control servers, this whole technology has a database which it maintains of first contact, last contact, commands, the name of the computer, the name of the logged-in user, all this information is sent back through just regular web queries in order to get this to the server which is controlling the network. So this stuff really exists. It is really happening.

And unfortunately, thanks to vulnerabilities in Windows, I mean, as far as we know all of this is Windows hosted. There's none of this that is nearly as well known or prevalent over on the Mac side, or Linux for that reason. But as a consequence of these vulnerabilities which are constantly being found, it's possible to use social engineering to get somebody to open a piece of email, maybe open a document, get themselves infected, put their machine under control, and in some cases these infections last years before anyone is suspicious.

Leo: Wow. Well, okay. Now let me tell you the story that I mentioned. This was in The Wall Street Journal yesterday. And the title, you should look for it, it's written by Siobhan Gorman, and the title is "Electricity Grid in U.S. Penetrated by Spies." The companies that run these grid computers, by the way, generally aren't discovering these tools. It's U.S. intelligence agencies, which are kind of chartered to protect us against cyber warfare, who come in and do assays and find this stuff. Tools have been left behind on many of these systems that could be used to attack and to take down the power grid. They don't make any assertions about who they're from. But U.S. officials said investigators have followed electronic trails of stolen data to China and Russia. It's kind of the same thing; right?

Steve: Yeah...

Leo: Both the Chinese and Russians deny it, as you would expect. So this is even more scary. I mean, it's one thing to get in an embassy computer and try to steal state secrets. But it's pretty clear that the next form of warfare will be cyber warfare. What's the first thing you do? You take down the grid. The grid goes down, a lot of what we do in this country stops.

Steve: Yeah, well, the Internet stops if you take enough of the grid down.

Leo: Right. You don't attack the Internet, you attack the grid, the power that runs it. The good news is that the effort is going on to be aware of this, to discover it, and to protect us against it. But I thought, this is just - it seems like another side of the same story, in effect.

Steve: Yeah, and all of this just, I mean, as someone who lives this technology, I mean,

who recognizes how easy it is to do these things today, it's wrong that it's easy as it is to do these things today. I mean, this all makes me feel like we're in the Wild West phase of, I mean, just the infancy of this technology. You know, I remember - I mean remember, not just stories of a time, I mean, I remember when there was the argument of, well, the Internet won't happen because of the chicken-and-egg problem. No one's on the Internet, so no one's going to want to get on the Internet. And it's like, whoa, well, that problem got solved. Now the Internet has happened. It's obviously here. It's obviously a huge win and a massive asset from an ability to leverage this kind of real-time communications and control and information flow and everything that we use it for. Well, it's not that long ago that no one really was taking it seriously. Now we are, but unfortunately all of the technology that we've got can be repurposed for non-intended purposes.

Leo: Yeah. And it's the same - really kind of stunning is it's the same holes that regular people are, you know, the same - these big government computers are falling prey in exactly the same way regular people are falling prey. They're doing the same dumb things, the same unpatched systems.

Steve: Well, because they're running Windows, of all things. I mean, I'm sure, Leo, you've seen the photos of, like, major light boards in Vegas that have a Windows error dialogue?

Leo: Blue Screen of Death, yeah.

Steve: It's like, oh, my God.

Leo: Well, I don't think running Windows, I mean, can't you harden Windows sufficiently? I mean, can't you make it secure? Or would it - what should they be running, if not Windows? You're running Windows. You must be able to secure it.

Steve: No, I mean, I'd use a nonstandard real-time operating system. There's all kinds of embedded operating systems around that no virus has ever attacked because it's not a target for anybody.

Leo: Or a NetBSD or, you know...

Steve: Yeah, exactly. I mean, when you see that, it just looks like amateur league. It's like, okay, fine. There was a...

Leo: Not just Windows, Windows 98.

Steve: There was some kiosk in an airport that I remember seeing where there was, I mean, they normally covered up the fact that there was Windows running underneath it. But it had an error, and up came a Windows dialogue box, right through this otherwise nice-looking turnkey - oh, and it was VB, I remember now seeing that it was Visual Basic

that they'd written this. It's like, okay. You get what you ask for.

Leo: Yeah. Wow. It's fascinating stuff. And a little scary at the same time.

Steve: Well, it's real. I mean, anyone - the thing I like about this story and sharing it with our listeners is this makes it so clear that it is this easy and that this stuff is real. This is not sci-fi. This is not...

Leo: Get your code on a hacker forum.

Steve: Oh.

Leo: That's what cracks me up. I had no idea this was just kind of commonly available stuff.

Steve: Yeah. Ghost Rat.

Leo: Ghost Rat.

Steve: Google it. Four clicks away, you've got the source code. And, if you're not quite sure how to compile it, well, just follow along in the forum.

Leo: Yeah, we'll give you binaries, yeah.

Steve: Follow along in the forum because they're all trying to figure it out, too.

Leo: Lots of helpful hackers, ready and willing. You probably get better support on Ghost Rat than you can get on most commercial software.

Steve: Oh, it's real-time, yeah.

Leo: Steve Gibson is at GRC.com. That's the website, Gibson Research Corporation. You'll find SpinRite there, the world's best file and - I'm sorry, disk recovery and maintenance utility. And of course a lot of free stuff, too, including ShieldsUP! and Shoot The Messenger, DCOMbobulator, Unplug n' Pray - I love his names - Wizmo. It's all at - and soon some new stuff, all at GRC.com.

Steve: Yup, coming soon.

Leo: Also there are show notes, 16KB versions for the bandwidth impaired, and Elaine's great transcripts so you can read along, as well, and pass it along. We have a wiki site with much of that stuff, too. I'm really pleased with the TWiT wiki. It's really moving along. Wiki.TWiT.tv. Thanks to all the volunteers who scribble, scribble, scribble while Steve talks. Thank you, Steve. We'll see you next week.

Steve: Right-o, Leo, thanks.

Leo: On Security Now!.