Ghostery

Description: This week, after catching up on the week's security and privacy news, Steve and Leo take a close look at "Ghostery," a highly recommended, multi-OS, multi-browser extension that reveals all of the tracking bugs and cookies websites are hosting to track us, and optionally allows them to be blocked.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-305.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-305-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 305, recorded June 15, 2011: Ghostery.

It's time for Security Now!, the show that covers your security and private online. And what would Security Now! be without the man who has been riding the horse, at the helm, skippering this ship since - for, what, six years now.

Steve Gibson: And watching it slowly sink.

Leo: No, no, no. Not at all. Mr. Steve Gibson.

Steve: Oh, the industry, I mean. The industry.

Leo: The industry's been getting worse. You know, it's so funny, I mean, we started this in, what was it, 2006? 2005. 2006. And at the time it wasn't as bad as it is now, was it.

Steve: It really wasn't. I mean, we didn't have an Attacks & Breaches section until recently. And now I'm thinking, how did we ever survive without one? Because, I mean, it's just - it's nuts.

Leo: Well, when we started it was really a show to teach you about topics and concepts in security, to talk about things going on. But we didn't do a lot of news.

Now it's at least half news because there's so much going on.

Steve: Yeah, and interesting stuff.

Leo: What is our topic of the day today? I see "Ghostery." What is that?

Steve: Yeah. This is something that a number of our listeners had pointed me to, that I had on my list of things to track down. And it is very cool. I would describe it as a comprehensive website surveillance monitoring and blocking add-on. The nice thing is that it's multiplatform and multibrowser so supports Internet Explorer, Chrome, Firefox, and Safari on all platforms. And it essentially - we've talked about cookies extensively, and of course even web bugs of different sorts, all these things that track us.

So I'm not sure why they call it "Ghostery." But it started off initially just being a monitoring tool. But its users said, you know, you're showing us all the things that are following us around and tracking us. Like you go to MSNBC, and it's just like, oh, my goodness, there's a list of eight different third parties which are participating at MSNBC's behest, tracking us. And Ghostery makes all of that visible, gives us lots of information about it, but now also allows us to block that.

So that's our topic for this week. I'm going to introduce our listeners to Ghostery and talk about its features and what I've found using it. And we've got a big Errata "whoops" at the top of the show about SD cards and write-protecting them, following up from last week's discussion. And I actually have probably the most controversial SpinRite testimonial we've ever had. So we're going to have some fun this week.

Leo: It'll be fun. And Marc Pelletier, who's in our chatroom, just told me that the Futures in Biotech show, which still feels to me like one of our newer shows, is five years old as of yesterday. So we've been doing this a while, Steve. It's funny how this network has grown and changed. And we were talking a little bit off the air about the new studio and the capabilities of the new studio. And what'll be interesting is that Security Now! won't look so very different. In fact, it will pretty much look exactly the same.

Steve: 'Cause I'm not going anywhere. I'm going to be right here in front of my bookcase with lights blinking behind me.

Leo: As will I, because we're duplicating this particular studio over there. So people tuning in in a month, which is about when we will start this change, will say, hmm, looks the same to me. And that's kind of what we want. We don't want to discombobulate you unnecessarily. It'll only be in the shows that need more production value than this show that we'll have that capability. And we may surprise you once in a while. We may have graphics fly in from the left.

Steve: Or monkeys.

Leo: Or monkeys.

Steve: Many of our very, very astute listeners immediately jumped on me via social networking connections, I think mostly Twitter, saying that what I had said about SD cards was wrong. And in retrospect, it was obvious that what I had said was wrong. So I wanted to immediately correct that. An SD card's little write-protect switch, which they all have as part of the spec for an SD card, as I did say, is just a piece of plastic. So in that sense, it's exactly like diskettes were in the old days, where you're relying not on electronics in the SD card, but in a sensing switch in the SD card holder to honor the write-protect request that the card is making via the position of that little bit of plastic.

Leo: So the reader is the key here.

Steve: Exactly. So...

Leo: But we said that, Steve. We said that a properly configured reader would honor it, but it would be possible to get around it.

Steve: But I was talking about an electrical connection that would be made. And, for example, I was correct in the USB side, which is to say, since the spec doesn't have write-protect, and there's, like, no means for enforcing it the way there is on an SD card, the USB devices are absolutely going to be an electrical connection because that's the only way to do it. But in the SD spec, they spec it as a switch which is readable, and it can be a function of the device driver to honor it. So you really do want to verify that write-protect is being honored by your system.

And I would argue that, if in fact, as I have been told, although I did not pursue it, it is device driver sensible, that is, the device driver can sense the setting of the switch and then choose or not choose to honor it, I know that's the case at least in some cameras because some people talked about how they've got firmware which they can provide on an SD card in some high-end cameras. And the camera can write to the card with the SD card set to write-protected, that is, to read-only mode.

So overall a better solution, if this is going to be what you're going to do, I would say trust a USB device. And the SD card advice is probably not - well, except in the case of an SD-to-USB adapter, where you want to verify that the adapter supports write-protection. But then it's not an option for the device driver to enable it or not, that is, pay attention to it or not. That would only be the case if the SD slot is actually hosted by the PC. If you're using an adapter, then the adapter's electronics, if it supports write-protection, it would be enforcing it there. So that bit of advice that we offered last week is correct with the strong caveat that you verify the adapter you're using does support SD write-protection. So I wanted to make sure we got that corrected.

We have just passed the second Tuesday of the month. And we didn't break a record this month for Microsoft's Patch Tuesday, but we're right up there near the top. They fixed 34 security vulnerabilities, 11 of which were in IE, and that spanned 16 different updates. More than half of those were critical, meaning by Microsoft's terminology that they are wormable, which means they require little or no user action in order to be exploited. And the rest were information disclosure and privilege escalation and so forth. So sort of our

generic large monthly update.

And I read somewhere something I really hadn't noticed before, but a commentator was saying that Microsoft tends to alternate bug sizes. So this was a big Patch Tuesday. And if this observation holds true, last month was - we know that it was small, but that would say that July will be small and August will be large. So we'll see if that's the case. I don't know why that would necessarily be. But we certainly do see that Microsoft has very small ones every so often. Not so this time.

Java we've been talking about a lot recently because, for example, in the case of Microsoft's own intelligence that they've collected from their rootkit scanning and malware removal tool that we talked about, they talked about how I think it was eight out of ten of the top vulnerabilities had gotten into users' machines through Java vulnerabilities. Well, Oracle has just updated Java to Update 26. So it's Java 6, Update 26. If you are using Java, and we've talked about if you know you don't need it, by all means remove it.

If you do need it - and there are an increasing number of instances where I'm seeing things require Java to be there, so I'm beginning to feel like, okay, we're losing the battle there. Although I did note that NoScript is able to control and corral Java also. So it's another one of the things that you'd want to have disabled on sites you don't trust, since, as I mentioned last week, since scripting is required to invoke a Java applet anyway. I know for example I've had to enable JavaScript in order to allow a Java applet to run on a site where I'm visiting for the first time. NoScript is also your friend in that regard.

They've fixed 17 vulnerabilities in this update. I had 25 before. Now I'm at 26. So if you've got Java, you really want to follow up on this because it's a serious way that is being exploited now to get malware into our machines. They fixed 17 vulnerabilities, all of which would allow code to be executed remotely without authentication. So these were big, bad holes. And nine of the vulnerabilities of that 17 were given a 10 out of 10 in terms of security risk, and that's Oracle's own ranking. And this update's available for Windows, Linux, and Solaris. Apple users will have to wait until Apple issues an update to address the flaws due to Apple's relationship with Sun and now with Oracle.

And I have to say I'm still annoyed that I have to say "no" to the Yahoo! toolbar that they're trying to stick in my browser and in my machine. That's just annoying. When I'm being forced to update Java because of security problems, and they're trying to hope that I don't remember to turn that thing off. Because it's on by default. That just - that really seems wrong.

Leo: No kidding.

Steve: Also, for Windows users, and I didn't look over on my Mac to see, but you can check the current version because there's a Java applet that you can get to on the Control Panel. So Start, Control Panel, then open the little Java applet, and there's a button you can click to do an "About" to see what version you've got. The other thing is, Java is willing to check for updates. And for some reason it's set to a month. And I thought, you know, Java being as big a problem as it is, even though Sun isn't updating it frequently, maybe if something really, really bad happened they would. So I'd like to have my computer checking more than monthly, which is the default. So I changed it. There's a tab there, you can change how frequently it checks. And I'm having it check daily because it's just a tiny little ping that's going to go out to Oracle to see if there's a newer version, so why not do it more often? I would say monthly, if you've got Java, and

it's enabled, is probably not often enough.

Leo: So I Googled "Java update." There is a Windows - is this what you're talking about? This is a Windows program that checks. But does this only check monthly? I think it checks all the time.

Steve: People can go to Java.com. So Java.com is where you get this. But for Windows it does, installing Java puts a little applet in the Control Panel that allows you to get to it.

Leo: That must be this Java Update, okay.

Steve: So last week we talked about Wednesday was the 8th, which was World IPv6 Day. And mostly it went okay. As I said, I would have more news this week, and that's what's happening. There were little implementation glitches, the kind of things that people would iron out and will iron out when they finally switch over. For example, some sites that were supporting IPv6, when they see that you're trying to get to them on what they consider a mobile platform, like a phone or an iPad, for example, they will redirect your browser over to their "m" - instead of www.something.com, it'll be m.something.com. I know I've seen that, for example, with Twitter and with various news sites. They'll give you a simplified, streamlined, mobile version that's more meant for a smaller screen.

Well, there were some oopses that occurred on IPv6 day because the "m" versions of their sites were IPv4 only. And so they had upgraded their www.whatever.com to IPv6. And so if an IPv6 user went there, they would be redirected to the m-dot version over IPv6, and that wasn't even available. So it's like, oops. That didn't work. So some mobile people found that sites they were trying to get to over IPv6 didn't work.

For example, there's something called MTU Path Discovery. MTU is Maximum Transmission Unit, which is basically packet size. And the way the Internet works, packets will be fragmented if they encounter a router that is unable to forward the packet to the next router without breaking it up in smaller pieces. For example, the router will know that the link that it's using is only able to handle, only able to carry packets of a certain size because of the limitations, for example, either at its end or at the other end. So it'll fragment packets.

But there are instances where packets have to be sent at a smaller size. So there's the ICMP protocol has always had this notion of path discovery, that is, a means whereby a router will send back an ICMP packet to the source of a packet, telling it, whoops, you need to make your packets smaller in order to get them through without them being fragmented. And in some cases fragmentation can't be used. So there were some failures there also, a week ago during IPv6 Day, where apparently some filters somewhere on the Internet were blocking the v6 version of this ICMP MTU Path Discovery packet. So they weren't ever getting back to the sender. The sender didn't receive the news that it had to reduce the size of its packets outgoing. And consequently people were unable to access sites that were, like, caught up in this problem. So that kind of thing.

The IPv6 traffic was way up for that day, but only relative to regular IPv6 traffic, which is almost nonexistent. So, yes, it was like many times more, but still minuscule. However, Facebook did put up a posting saying that their test went very well. And I think it was 0.03 percent of their users came to Facebook over IPv6, which was a million users that

day.

Leo: Isn't that funny, it can be such a low percent and such a high number?

Steve: Yes. If you're something like Facebook, that's the case. And one of the other observations was that a huge amount was tunneled IPv6. We talked about tunneling IPv6 the other day, the idea being that you could encapsulate IPv6 protocol in IPv4 packets in order to route it across the IPv4 Internet. And that's what - still a vast amount of traffic had to go through tunneling, which tells us that major portions of the Internet are still to this day, as we're counting down the end of IPv4 space, still unable to transit IPv6 traffic. So, I mean, we're really not here yet.

Also and finally, a few participants, such as, for example, Xbox.com, had everything go so well that they're keeping IPv6 addresses in DNS.

Leo: Wow.

Steve: And that's actually the way sites like Xbox.com and Facebook and Google and Yahoo! and others, that's the way they did this was they added IPv6 DNS to their existing IPv4 DNS, so that a query for DNS would receive IPv6 records in addition to IPv4, thus advertising the fact that here's, if you want IPv6, here's our 128-bit address for accessing us. And Xbox.com said, yeah, we're going to leave it because it all worked really well. So that's cool.

I did get some listeners telling me about a site which probably happened or at least got some news just recently called Encipher.it, as in Encipher It, clever name in the .it top level domain. It uses bookmarklets and offers bookmarklets for IE, Firefox, and Chrome, which performs an in-browser AES encryption of text that you paste in. So its sort of an add-on, for example, for web-based mail. You could put in a bunch of stuff that you want to encrypt, and then mark it and give it a passphrase, and it will do an in-place encryption.

Now, it's cool, but there's one caution that I have. And this is not something I have pursued yet, but I intend to. And that is that, as I understand it, bookmarklets run in the context of the site that you're visiting. And it's one of the reasons why I'm a little cautious of the gizmo you use, Leo, I can't remember the name of it now, but you'll know. The thing you use for generating passwords based on the sites you're visiting. Help me out here.

Leo: LastPass.

Steve: No. No, no. It's something that you...

Leo: Oh, SuperGenPass, you mean.

Steve: SuperGenPass.

Leo: Yeah, yeah, yeah, yeah, I use that. I still use that. But I do the padding that you now recommend with haystacking.

Steve: Okay, good. Because there's some concern about SuperGenPass's security, inasmuch as it is similarly a bookmarklet-based deal.

Leo: Yeah, it's JavaScript.

Steve: And what I've seen is the claims that an untrustworthy site can compromise its security. That is, bookmarklets run in the context of the site you're visiting. So I would trust Google, but there are TNO people who perhaps wisely trust no one because...

Leo: But could they reverse - so what happens, what they'll see - would they see my master password? Because that would be the only risk there.

Steve: Yes, potentially.

Leo: Okay.

Steve: Yeah, they have access to the script, as I understand it, which has access to your password. Again, I haven't had a chance to research it fully. But I did want to let people know that if they're wanting to do encryption, it's a cool idea, but you are trusting the site you're visiting. And you're also trusting that nobody has inserted any scripting on that page. So you want to be doing it over HTTPS for sure, as well. And I intend to pursue this because I'm interested in finding out what the security dangers of bookmarklets are. That would be a great topic for a podcast.

Leo: And if I add padding, arbitrary padding, and it could be the same on each site, that's going to obviate their ability to figure out what's going on.

Steve: Yes. They would not be seeing that, yes. Also a bunch of people noted that - this hit the news, the security news this week - that LinkedIn, Foursquare, and Netflix had been found by a security auditing firm to be storing their passwords for Android phones - and we're not sure about iPhones, but all these same companies offer iPhone apps, as well - were storing their passwords in plaintext text files.

Leo: And probably sending them in the clear, I would guess. I wonder.

Steve: It was not clear. Foursquare has since updated their Android application. And I just have to shake my head, the idea that in this day and age applications could be that dumb, I mean, could just be that lackadaisical about their users' security. And, now, someone might say, well, okay, but what's the big deal about my username and password for Netflix, except that we do have the problem that many people reuse

username and password elsewhere. And so you really don't want some compromise to get a hold of that information out of your phone and see if they're able to log in, well, first of all, you probably don't want them logging into your Netflix account or any other account.

Leo: They could watch my movies.

Steve: Or LinkedIn or whatever. But...

Leo: I think that would be the bigger risk, is if you use the same password everywhere. Which I don't. And people should stop doing that in general.

Steve: Yup, and I'll have something to say about that before long, too. IE and Firefox are both losing market share to Chrome and Safari, which are both gaining market share. I just thought I would - I saw a nice little blurb, I thought I would just sort of give us an update on that. Even though, okay, we have new versions of IE9 and Firefox v4, soon to be v5. Firefox users are upgrading from their 3 versions up to 4. IE users largely are not. We're not seeing much rapid adoption of IE9. Most IE users are staying with 8. And 10 percent of IE users are still on IE6. So, which Microsoft is beginning to get upset about and, as we talked about previously, beginning to launch a campaign to get people off of IE6.

So at the moment IE is still the majority browser. It has 54.27 percent of market share. Firefox is in No. 2 place at 21.7. Chrome is in third place at 12.5. And Safari is at 7.25 percent. And Opera dropped a bit. They're down at 2 percent. But what this means is Chrome is currently the only browser now seeing consistent month-to-month gains. So Chrome's share is coming at the expense of every other browser. Firefox users are holding on. They're loyal, as I am. But people who are adopting Chrome are leaving IE and Opera. And Safari's share is gaining just because of Mac market share gain that brings Safari along with it. So I thought those were some interesting statistics.

And one last little bit of security news, it turns out that the new Nissan LEAF, which is the Nissan EV, is sending its location constantly. It comes with a GSM cellular connection to the Internet - it's one of the sort of built-ins for the car - which provides voluntary telemetry information to Nissan and also, for example, is used to provide, like, to update the in-car map with the location of new charging stations as they become available. And there are some, like, wacky competitive driver rankings where you can see who's able to, like, drive, then get the greatest battery mileage. And so you can participate in a network to compete with drivers to see who can be softest on the gas pedal and economize the most on electricity. But it also offers RSS feeds. That is, you're able to configure it to receive news from anyone who's an RSS provider. And collectively this thing is called "CARWINGS," is the service.

Well, what Nissan never discloses and has no way of allowing their users to disable, although I imagine there'll be an update coming soon, is that every RSS query, which is a standard HTTP "get" query, and we've talked about how "get" queries can have headers, the headers are just chockful of information that drivers may not want sent because RSS feeds are constantly, sort of a constant background polling for any news. With that your current latitude and longitude is sent, your car speed and compass direction is sent, as well as the destination latitude and longitude configured into the navigation system.

Now, to mitigate that concern, there does not appear to be any unique car information. So it doesn't look like you individually are identified. But anyone - and I could see it as a benefit, if it was optional, where, for example, you might get location-based weather. So if you wanted weather updates, it would know where you were, and the weather service could check to see what was going on near you, or regional news and so forth. Yet it ought to be disclosed, and it ought to be something that you're able to suppress, which currently is not available on the LEAF. So it's like, okay, well, these are lessons we're still apparently learning.

In Attacks & Breaches, we've got a widely publicized and, I guess, significant breach of the IMF, the International Monetary Fund. Little is known still about what exactly happened. It appears that attackers were able to get software on a computer that was persistent for some length of time which allowed them to access the IMF's network and reportedly exfiltrate a large amount of data. It's believed that this was preceded by a targeted spear-phishing campaign. And Bloomberg reported that the attack appears to have been mounted by a foreign government, although no specific country was named. And Bloomberg's unnamed source also stated that the IMF lost, quote, "a large quantity" of data. And the bad news is that much of that data is extremely sensitive, dealing with the internal financial state of various countries' economies and the state of their negotiations with the International Monetary Fund.

Leo: That's not good.

Steve: So sensitive stuff got loose in a big breach. Also Citi, as in Citibank, but Citicorp disclosed that earlier last month - and people are a little upset that it took Citi so long to tell us - as many as 210,000 customer names, email addresses, and account numbers and contact details were lost. But Citi said that the associated PINs and the card security codes and other data aside from names, email addresses, and account numbers existed on different systems and were apparently not breached.

Not much is known about the attack. But I did read one report which indicated that the hackers were manipulating the URL of, like, while logged in, as if to say, and one account did say, that the actual account numbers were in the URL query. So just by changing the queries, they were able to get into other people's accounts. Which sounds really screwy, but...

Leo: Oh, that's wrong.

Steve: Really wrong. And people apparently in the know are saying that Citi's security was virtually nonexistent. So it does sort of sound like it may have been that dumb. And we've talked about the dangers of putting sensitive information in URLs because, remember, any third parties that were presenting information on Citi's site received that URL in the so-called "referrer field."

So we'll know when we're talking a little bit later about Ghostery, if you go to Citi.com, Leo, Ghostery will show you all the third parties which are putting content on that site. And if they're also putting content or trackers on the sites where those account numbers occur, they would be receiving the account numbers of the users in addition to their IP addresses and so forth. And they're all about aggregating information. So really you don't want to leak account numbers in URLs. That's - there's all kinds of bad things that can happen. I mean, that's, like, second and third order effects from that.

Leo: It's actually listed, from OWASP.org, one of the top 10 insecurities on the web. I mean, it's, like, well known and easy to fix. And it's just ridiculous. That's just ridiculous.

Steve: Yeah, and we just keep seeing over and over instances of very lax security. And I'm hoping that enough attention is being brought to this, as I've said before, that people will start fixing this stuff preemptively. I mean, instead of it just getting on the web and everyone screams with joy that it's working, yeah, but is it working securely, is the question. And the U.S. Senate.gov server was breached. They have said that only that one server was breached, and it only contained content for public consumption. So no sensitive information got loose. But it was the LulzSec group which have claimed responsibility for many of the Sony breaches and Nintendo and the PBS breach recently, were the same folks who did this one. So those guys are getting around.

And I've actually seen some interesting commentary where security researchers are saying, yeah, well, we think it's really bad that these guys are so successful in breaching sites. On the other hand, this is what's giving companies a wakeup call that they may be next. And so fix yourself before you suffer a big black eye from having an outfit like this LulzSec breach your company.

And I picked up on a piece of news following up from two years ago, a report that we discussed, actually maybe it's three years ago. No, two. I saw both SANS and Brian Krebs reported. Our listeners may remember we talked about it. In May 2009 a company called Patco Construction, they had cyber thieves, as they called it, used the Zeus Trojan to steal their online banking credentials - and this is known, this was reported two years ago, in fact we talked about it - and transferred $588,000 in batches of fraudulent ACH, the automated clearinghouse transactions, over the course of a week, over seven days. So Patco sued their bank, claiming that the bank's security was insufficient for their customers' protection.

In the weeks that followed that original breach, the Ocean Bank, which is the bank that was sued, was able to recover $243,000 out of that $588,000, but that still left $345,000 that Patco ended up bearing the loss for. So this is significant today because just recently a magistrate in Maine recommended that the court make Patco the loser in this suit by denying Patco's motion for summary judgment and granting the bank's motion that the case be dismissed. It's believed to be unlikely that the judge in the case will overturn the magistrate's findings. So here we have a case where, I mean, with a lot of money involved, where a company who suffered a breach as a consequence of a trojan that was in their machine, captured their online banking credentials, which is username and password, and actually even a security question.

I dug into this a little bit deeper, and it turns out that what happened was the bank, Ocean Bank, used to have a system in place where, for transfers over $100,000, one of three security questions was asked. And it was by having that in place that the bank was able to say they had multifactor authentication. Well, what happened was they were having so much problem with much smaller transfers that they dropped that $100,000 limit to $1. So almost all transactions, well, virtually all transactions, anything at a dollar or above, would be asked a challenge question. So what that of course meant was that the challenge question was being asked all the time.

So the Zeus trojan was able to capture the questions and the responses from much smaller payroll transactions that this Patco Construction was doing and then be able to log-on on behalf of Patco Construction. So the result of all this is that the bank is not

being held liable, and there is zero case law until now, and what the case law we have is that, if a company gets hacked in a way like this, even a username and password and additional protection which ends up being breached is the fault of the customer, not the bank.

So I wanted to use this opportunity to reiterate what I have said a couple times, which is, if you're a small business, or even an individual, and you do not need to be doing electronic funds transfer with some of your accounts or any of your accounts, disable them. You can tell your bank you want to disable that feature. And I have on all of ours. And Sue, my operations gal, is forced to walk checks around. But there's just no way I'm going to allow this kind of a breach to drain GRC's money out of us, and then for there to be no recourse, that money is gone, and if it can't be recaptured electronically, which in this case some of it was, it's my loss.

So my feeling is, sorry about that, this technology, we just don't have enough security yet today to make this kind of major account access available electronically for it to be safe. So we're still using paper. And if the bank then makes a mistake and does honor a charge, when we have explicitly told them not to, then they absolutely are liable for it. So that's where I want the responsibility to be.

There was an interesting, in our Miscellany section, an interesting survey of iPhone passcodes. We've been talking about passwords recently, so I thought users would get a kick out of knowing that the number one most popular passcode used on iPhones, you probably can't guess it, Leo, or maybe you probably can.

Leo: Monkey?

Steve: Monkey. These of course happen to be numeric because the iPhone has a numeric keypad. So the number one passcode is 1234.

Leo: I could have told you that.

Steve: That's what people use to protect their phones. And number two is 0000. Then for some reason comes 2580. And I'm not sure why. I looked at the keypad, it's like...

Leo: Straight down or something?

Steve: It's up the center and then down to the bottom. So, yeah, so it's 258 are directly vertical, and then down to the bottom. The fourth most popular is all ones, 1111. Then comes all fives, 5555. Then 5683. And I'm not sure what, let's see, 568 - that's a kind of a strange thing. But a lot of people use 5683. Then 0852.

Leo: It spells "love," somebody said.

Steve: Ah.

Leo: Is that true?

Steve: 5683 on a phone pad? I don't have one near me.

Leo: Don't you have that memorized? Apparently somebody on my staff does.

Steve: I'll bet that's the case. And, okay, how about 0852?

Leo: 0852, what's that?

Steve: "0" doesn't have anything, that's just operator.

Leo: Huh. Is it going up? Yeah, it's going up. It's going up. So, see, if you look at it, that's the key. If you look at it, 2580 is going straight down the middle, and 0852 is going straight up the middle. That's why.

Steve: Okay. And then we've got 2222, 1212, and 1998. And it was interesting, they did a breakdown of the 1900s. And it looks like people are using, based on demographics, the expected demographics of iPhone owners, they're using, like, their graduation dates, or maybe their birthdates.

Leo: Or maybe the current year, and it just happens to be that that's the one that's been around the longest; right?

Steve: Well, no, because we haven't had iPhones...

Leo: Oh, wait a minute. You're right, it would be 2007 that it came up.

Steve: So there's a huge peak, like in the late 1990s.

Leo: It's 22 year olds. There are a predominance of 22 year olds or 23 year olds on iPhones.

Steve: Probably year of birth. And then there's been some news about Bitcoin which I wanted to share just because it's sort of interesting to see what's going on with Bitcoin. The largest bitcoin holder has, or had, well, I'm not sure because there was a break-in. Someone lost their bitcoins. You and I were talking about it before we began recording the podcast. I heard that it was a half a million dollars' worth. I don't know when that was because bitcoin currency exchange rates have been fluctuating a lot lately. But the largest bitcoin holder has 297,000 bitcoins.

Leo: Wow, that's a lot.

Steve: That's a lot of bitcoins.

Leo: I mean, at what, 20 bucks a pop?

Steve: $31 last week, $9.2 million worth of bitcoins.

Leo: If you could find somebody who would buy it.

Steve: Well, but there's an active brokerage. Now...

Leo: Yeah, but I doubt you could unload 200,000 bitcoins on it.

Steve: Well, okay. Here's some stats. The MtGox.com exchange, which is the largest bitcoin exchange, has been charging 0.65 percent as a brokerage fee. A few months ago, that was only minting it pennies a day. Last Wednesday it was making $40,000 a day.

Leo: What?

Steve: There's that much bitcoin transaction. In one day, $2 million of bitcoins were traded in 5,871 transactions.

Leo: That's surprising.

Steve: So this is really going on. Now, what did happen was that last Friday Bitcoin suffered its first depression. It was called "Black Bitcoin Friday." At the opening of the day, bitcoins were trading at $28.91. By midday that had dropped to $20.01, a drop of 30.8 percent over the course of half a day. And I have to say, I mean, I talked about it last week. We noted that I have 50 bitcoins, and at $30 each, that was 1,500 bucks. And I was tempted to say, huh, maybe now would be a good time to cash in my 50 bitcoins.

Well, apparently I wasn't the only one to think so. I did not cash them in. I still own those 50 bitcoins because it'd be kind of fun to see what happens. But many people must have decided that, whoa, 30 bucks a bitcoin? I'm taking my money out of this. And so of course the consequence was it drove the price down over the course of a day. So it'd be fun to see where it goes in the future. But, I mean, it really is happening, Leo. I mean, money, serious money...

Leo: According to Mt Gox, it's currently 19 bucks, I think. So you should have sold.

Steve: Well, who knows where it's going to go? We'll see.

Leo: But this shows how much speculation is going on.

Steve: Well, speculation and trading. I mean, people, if you're trading $2 million a day and nearly 6,000 transactions, I mean, there's actual money that is being exchanged anonymously, as it was designed to be, through bitcoin.

Leo: Yeah. I think it's when it's this volatile, I have a feeling that's a sign of speculation. Of course, as soon as it hit the low on Black Friday, it peaked up almost to its all-time high as people bought them up.

Steve: Bought them up again.

Leo: Then there was a minor selloff, back up, a bigger selloff, back up, and now it's kind of stabilized right around 20. It's interesting.

Steve: Yeah. Okay. So the most controversial SpinRite testimonial we've ever had. I think I'm going to leave this anonymous.

Leo: Okay.

Steve: Because he didn't ask me to, but I think I should. So the subject was "SpinRite rescues some pictures, and a question of etiquette." This was sent from Daventry, England on the 27th of May. He says, "Hello. I'm a regular Security Now! listener, and I'd like to share this story with you. I'm always on the lookout for broken computer parts. When a friend's laptop broke down, he asked me if I wanted it, which I did. In the conversation he told me he was a little depressed as there were lots of unbacked-up photos on the laptop. He had done 'everything,' in quotes, to try to rescue the files, but he had lost all hope of recovering them." Well, we know where this is headed.

"I wondered if 'everything' included SpinRite, but decided against asking as I didn't want to depress him or get his hopes up. Instead, I gave the laptop to a friend, a fellow Security Now! listener, and asked him to try his copy of SpinRite on it. Next day he reported that it worked, but warned that the disk was not long for this world, and I should make a backup while I still can." Which of course is one of the things that SpinRite will tell you. "Buzzed for a chance to be the hero, I booted the laptop up and prepared to copy the files onto a USB hard disk. Not knowing where his pictures were, I browsed into the My Pictures folder and found myself looking at some very pornographic pictures of my friend and his wife."

Leo: Whoa [humming].

Steve: "I quickly made a copy of the files..."

Leo: Yeah, close your eyes and move on.

Steve: Uh-huh, "...slightly embarrassed at what I saw. He must have been really convinced the contents were gone for good."

Leo: No kidding.

Steve: "Now I'm not sure what to do. He didn't ask me to recover the files, but I know he really wants the pictures back." I guess those he can make some more, but probably other pictures, too. "If I give him a copy, he'd know I must have seen them. Any advice?"

Leo: Yeah. Hmm. That's one for The Social Hour.

Steve: That's a tricky question.

Leo: Dan Savage, maybe. Boy, I don't know, that's a really interesting question, isn't that.

Steve: It's an ethical dilemma. SpinRite recovered the pictures, which were believed to be long gone, and, ooh.

Leo: It worked too well.

Steve: Yeah, there was a reason that drive was overheating.

Leo: All right, Steve. We are ready to get underway here with Ghostery. I have installed it, and I'm going to sites and shocked.

Steve: Well, I'm really impressed with it. It's a free add-on for IE, Firefox, Safari, and Chrome, so all the major browsers on all the major platforms. I used it over on a MacBook Air yesterday and on my PC today. And what it does is it is watching the web pages that are watching us. And in a very innocuous, just sort of "oh, by the way" fashion, shows users who visit sites what third parties are tracking them.

So, for example, I go to MSNBC.com. And in the upper right-hand corner of my browser window - and that's user configurable, you're able to change how long the window stays there. If you click it, it disappears immediately. Also where it pops up, so there's plenty of configuration settings. But MSNBC.com, if I hover over the toolbar tool, it says "7 trackers found on this page, and 7 blocked." And then it lists them: DoubleClick, DoubleClick Spotlight - yeah, because DoubleClick didn't have me in enough of a spotlight already, so we got the second, DoubleClick Spotlight.

Leo: These are ad trackers.

Steve: Yup. Insight Express, Microsoft Atlas, MSN Ads, Omniture, and Pulse 360. Now, what I like about this - well, I like everything about it. I recommend it for anyone who's curious. I mean, even just run it for a while just to sort of see what's going on. It's just really innocuous. And the blocking is optional. But if people want to use it for tracking blocking, you absolutely can. when you install it, it asks you three questions. It asks you if you want to enable GhostRank, which is disabled by default, that is, so that's opt-in. And it explains that enabling GhostRank will allow you to anonymously participate in an information-gathering panel designed to improve Ghostery performance and create a consensus of advertisements, tracking beacons, and other page scripts across the web. The data collected is used only in aggregate, contains no personally identifiable information, and will never be used to target advertising.

Now, I did enable it. And one reason I did is one of the things that they'll show you, and I'll explain where here in a second, is, for example, what sites have these particular trackers. So, for example, you're able to drill down and say, okay, what's Omniture, and get a really nice, very even-handed description of all of these things. And you can get that by clicking on the Toolbar button. Then it'll relist for you everything that it found. And from there, there are submenus where you're able to go in and bring up a page from Ghostery's own directory that explains in very good detail what's going on, what the company does, what their policies are, what informative it is that they collect and so on. And on that page it also shows, for example, here's a bunch of the sites which have this. Well, the only way they know that a bunch of these sites have it is if the users of this product allow their browser to send that information anonymously back to the Ghostery folks. So anyway, I turned it on.

So this continues to say, "When you encounter a script and have GhostRank enabled, Ghostery sends a record that includes the following: the page elements identified by Ghostery; the elements blocked by Ghostery; the number of times the element has been identified; domains identified as serving those elements; advertisements served at particular domains, including companies associated with each ad; the information about the type of notice associated with each ad; the browser in which Ghostery has been installed; and the Ghostery version number." So that's something you do not have to do. But if you do, it increases the accuracy of their database. So I liked the fact that it was opt-in.

The next feature, after you select that, enables an "alert bubble," as they call it. It's that little window that I talked about which pops up, which I enabled. Again, you can disable it later. You can change how long it stays up. And I think it defaults to 10 seconds, or maybe 15 by default. So you're able to just sort of glance at it. And if nothing else, you can see how long it is quickly because some sites only have a couple; some look like a dictionary of every nightmare that you ever saw. And then they maintain this notion of "web bugs," which are all the little either ads or tracking beacons or bugs. And when I installed it, there were initially - it knew of 518 different companies that they had encountered who were installing these on my machine. And out of that 518, 345 also were planting cookies on my machine. So not all, but certainly the majority.

Leo: It's really nice to have that information. But what you'll find immediately is that many, many, many sites have this stuff on there. I was just looking at TWiT.tv because I didn't know what we use, and we only use one thing, a little "Add This"

button.

Steve: Yes, I did see that. I went to TWiT.tv also and saw that. And, yeah, it's just, I mean, it's sitting there on the side. It's not in your face. I mean, it does proactively block. And in fact, in one of their early blog postings, a user asked the question, "Does Ghostery stop the tracking process?" And I really liked their response. They said, "It's an option, but most of our users like to allow some page elements and disallow others. The free content on the Internet is paid for largely by advertising, and data collection is part of that. We don't want to deprive publications or advertisers of their revenue. That would be bad for the content on the web. But we do want our users to know who is collecting their data and control it wherever possible. How much data collection a person will tolerate is up to them. It's their own subjective decision, and we would never try and make that on behalf of others."

So this is very comprehensive. For example, I went to their own blogging service - they use a third-party blog. And I thought, well, who's - and when I went to that page, up came the little balloon window that had three entries. It had Facebook Social Plug-ins. It had something called New Relic, and then Twitter Button. And so I'm able to explore into those by using the toolbar. And I should remind people that that isn't made visible, the toolbar button is not made visible automatically, at least in Firefox. I had to right-click on the toolbar and then hit Customize and then drag the little ghost, it's a little ghost icon, looks a little like a blue Casper, up onto the toolbar. And it has a nice presentation under Safari and Firefox on the Mac.

And the button, even though the little balloon goes away, there's a little sort of highlighted number on the button to sort of remind you, you can just look, and I remember seeing a "7" when I was on MSNBC because there were a total of seven different things that were tracking me on MSNBC. So you're able to, by company, you can enable or disable all of those cookies and tracking. And then separately you're able to whitelist individual domains where you want to allow all of that to go on.

Now, the one caveat for people who are NoScript users is that many sites use their scripting in order to bring their third-party trackers onto the page. So if you are already blocking a page with NoScript, then NoScript has prevented the tracking activity, and Ghostery won't see it. So I found that sites I'm not trusting, Ghostery will see some things. If I then deliberately trust them, Ghostery will see more, meaning that the scripts which I'm then allowing to run are responsible for exposing these additional trackers. So there is some interaction between NoScript and Ghostery.

But overall, I just think it's a great little app. I played with it for a while. I poked around. I'm going to run with it now on my browsers. I know there are people who just wouldn't be into this at all, they're just going to use the web and not worry about it. There's another class of people who might want to be informed, but not block because it's just sort of additional information. And it's the kind of thing you might want to use for a couple of months and then decide, okay, now I have an intuitive sense for how much of this is going around. Or there are certainly another class of people that like the idea of just flatly blocking everything, even on sites that they trust with NoScript. So that's one way that these two work nicely together.

I normally am trusting MSNBC.com. I've got that permanently allowed in NoScript, which is why I'm seeing all seven of these things come up and track me. But I want to block the tracking, thank you very much. So Ghostery allows me to do that. So I think it's just an across-the-board cool little add-on for our browsers - multiplatform, multibrowser. It's

out of the way. You can uninstall it later if you get tired of the information, or you can leave the tracking enabled and disable the popup balloon. And then all you get is the little number on the little Casper ghost on your toolbar, if you decided to have the button there. But it can also operate as a completely invisible blocker of all these web bugs, 557 of them at last count.

Leo: What page has the most that you've ever seen?

Steve: I think MSNBC might be up there.

Leo: Oh, I could beat that.

Steve: What's Disney.com look like?

Leo: Yeah. I just went to a nonprofit site. I was looking up a Senate bill we're going to talk about on TWiG this week. It had 17. GovTrack.us, which is a great site, has 17 on there. So, yeah, that's a good question. Let's see what Disney has. I think what might surprise you is that - and this is probably why it's fun to just browse around with this turned on for a while, just to see what you could see - is that you may be surprised by the number of sites you wouldn't expect. Wikipedia, as far as I could tell, had none, which was good.

Steve: Yup. I did go to Wikipedia, and it was a big zero, which is just beautiful. So that site is pulling revenue from those 17...

Leo: Not necessarily. I mean, a number of these - Comscore Beacon, Google Analytics, Quantcast - are merely measurements. They want to see tracking.

Steve: And Google Analytics, by the way, is all over the place. I had a hard time finding a site that didn't have Google Analytics on it.

Leo: And we use that. Facebook Connect is designed to make it easier to log in. But then there are a number of ad networks. You know, it's interesting, Disney only seems to have two. Microsoft Atlas...

Steve: I see that a lot, too. What the heck is that?

Leo: Well, I wonder if that's a - it's an ad center. So it's another - it's a Microsoft ad system.

Steve: Okay.

Leo: You're going to see a lot of these. I mean, let's face it, the Internet is free. And that's often how you pay for a site.

Steve: Well, again, it's one thing to see the ads, and another thing to have information sent back. And Ghostery does follow up. I mean, if you, like, click on Omniture and dig down, it'll say this is the information that they're collecting, and it'll give you a link to their privacy policy. I mean, so it really allows you to do some research beyond just enumerating how many things have been loaded on there to follow you around the Internet.

Leo: Happy to say EFF.org, which you would think would not have a lot of privacy intrusions, has zero.

Steve: Nice.

Leo: That's how it should be. It's kind of interesting. You get to be the judge. That's the point. This is information that you can use and you should use and be aware.

Steve: I think it's very nice browser instrumentation that can be used to block, to inform, to entertain, and also to educate a lot because, I mean, there's no doubt that users, our listeners, are going to be interested in this, are going to install it, and are going to spend some time digging down, saying what the heck is this company? Pulse 360, okay. And then decide, yes, I like that; or no, let's keep it on the block list. Because you can tailor this exactly the way you want to, also.

Leo: People are asking about live.twit.tv. We have three trackers on there, and all of them are used to - actually I don't know why we have AdWords on there. I don't think we use AdWords. But we do have Google Analytics and Quantcast on there. And those are - I think Chartbeat's on there, too.

Steve: Well, so that's kind of cool, too, because now that reminded you that maybe you should remove the AdWords script.

Leo: Yeah, why is AdWords on there, yeah. I don't think we use that. Maybe that comes with Analytics, I don't know. And we use Quantcast. And I thought Chartbeat was on here, as well, which is another monitoring service, because it's a way we have of - yeah, there's Chartbeat. It's a way we have of...

Steve: There's that little...

Leo: Actually that's all we have is Chartbeat, Google Analytics, and Quantcast. Those are the three that are on there. And that's all traffic measurement. Now, some of them do leak information. Some of them don't have a policy about that, and so

that's - maybe this will also stimulate people to update their policies.

Steve: That would be great.

Leo: Yeah, yeah. Good stuff. I like this plug-in. Steve, we're done, I guess, I gather.

Steve: We're done.

Leo: A great show, as always. If you want to know more about all of these topics, the place to go is Steve's website, GRC.com. That's where you'll find, of course, a copy of the great SpinRite, the world's finest hard drive maintenance and recovery utility. You'll also find lots of freebies that Steve gives away, and a place to ask questions of Steve that we use on every other show. In fact, next week is a feedback show, so GRC.com/feedback for that. Also his Password Haystacks article from last week, that was great, or two weeks ago. That was great stuff.

Show notes, 16KB versions, full transcripts of all 305 shows, it's all there, GRC.com. We do this show every Wednesday morning, 11:00 a.m. Pacific, 2:00 p.m. Eastern, that's 1800 UTC, at live.twit.tv. And you can watch us live, or you can get the show after the fact at Steve's site or TWiT.tv/sn. Steve's on Twitter, @SGgrc, that's the place to go.

And don't forget, we are still selling bricks. In fact, we're getting close. I think we're about a month off from moving into the new studios. And if you want to have a brick on the wall with your name, your Twitter handle, your Facebook handle or whatever, just go to bricks.twit.tv. That Wall of Honor is looking so cool. Literally, the honor's all mine. It's really amazing. Bricks.twit.tv. Did you get one, Phil? He wants to buy one. All right, he's giving me a credit card. I can't take credit cards, but we'll figure that out.

Hey, Steve, thank you so much for being here. We really appreciate it. And we will be back next week, same time, same channel, for more security news on Security Now!. Bye bye.

Steve: Thanks, Leo.