The Internet Underworld

Description: We first converse with today's special guest, Brian Krebs, who for many years wrote for the Washington Post and is now publishing his own "Krebs on Security" blog. Our topic is "The Internet Underground." After that, we catch up with a somewhat busy and interesting week in Internet security.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-392.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-392-lq.mp3

SHOW TEASE: It's time for Security Now!, and we're in for a big treat. One of my security heroes - not Steve Gibson. He's here. Actually two of my security heroes are on the show today. Steve, yes, but also Brian Krebs. He started writing "Krebs on Security" when he was at the Washington Post. He's been doing it on his own for the last three years, KrebsOnSecurity.com. Brian Krebs talks about The Internet Underworld, next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 392, recorded February 20th, 2013: The Internet Underworld, with Brian Krebs.

It's time for Security Now!, the show that covers your security and privacy online with this fellow right here, our Explainer in Chief and security guru Steve Gibson of GRC.com. Usually it's just Steve. It's the Steve show. But today we've got a guest.

Steve Gibson: Yeah, we do. I refer to Brian often on the podcast because he has his thumb on the pulse of a different aspect of security than we normally cover. When I approached Brian about being on the podcast today...

Leo: I should say, because you keep saying "Brian," it's Brian Krebs.

Steve: Oh, yes.

Leo: Who has, for many years - welcome, Brian, it's great to have you on Security Now! - for many years wrote about security at the Washington Post and really brought a well-informed eye on security to mainstream media, which was kind of

unusual. In fact, no one's doing it after you left. Hard to believe it's three years ago, and now doing it on your own at KrebsOnSecurity.com.

BRIAN KREBS: Yes, sir.

Leo: Great to have you, Brian.

Steve: Yeah. And as I said, I often refer to Brian. I keep an eye on his blog. And what I see is that he sort of has a different focus than we do. We're more sort of security technology and security theory and sometimes computer stuff and that. Brian's take, from what I've seen, is to, like, watch what is going on by all the cretins.

Leo: [Laughing] Cretins?

Steve: Cretins.

Leo: Smart cretins, though. And they're not from Crete.

BRIAN: I like to call them "miscreants" in my - my friends who read my stuff a lot say - they tease me, and they go, you know, Brian, we'll give you a dollar every time if you just replace "miscreants" with "ne'er-do-wells."

Leo: Ne'er-do-wells, I like that even better, yeah.

BRIAN: Yeah.

Steve: And that's better than trying to figure out what color someone's hat is because...

Leo: Black or gray or white, yeah, yeah.

Steve: ...you know, is it gray, is it black, is it dark gray, is it light black? Who knows what.

Leo: And it's better, more importantly, than the word "hackers," which has a...

BRIAN: Right.

Leo: You know, while mainstream media - and for some time people said let's call them "crackers," which didn't really sit well with me. It sounds like somebody on a

porch playing a banjo.

BRIAN: I have a theory about that. If somebody calls a malicious hacker a "cracker," they've just dated themselves. I mean, that's - but he's been around the scene for a long time and really takes offense at the hackers...

Leo: And hackers should really have - but "hackers" should have a more honorable tone to it, since it does have an honorable beginning. And there are still many hackers out there, hardware and software, who are not miscreants. So I like "miscreants." "Ne'er-do-well" is even better. Bad guys.

BRIAN: There you go, bad guys, yeah. That's...

Leo: And I hate to say "cretins" because I don't think they're necessarily dumb. Some of them are dumb, but there are some very impressive cretins out there, as well.

Steve: Okay.

BRIAN: Without a doubt.

Leo: Yeah.

Steve: Now that we've established that.

Leo: Nomenclature is important, Steve. You know that.

BRIAN: Words matter.

Steve: We're going to have fun this podcast - oh, nomenclature is everything - talking about Brian's focus, that is, what the bad guys are doing, what the trends are, what sort of - there's, like, state sponsored. There's organized crime. There's random individuals. How does the money flow? Just sort of take an overview of this aspect of what goes on with Internet crime in general.

BRIAN: Yeah.

Steve: Which is not something we've spent much time talking about, and that's where Brian spends a lot of time looking. So I thought it would be great to get his thoughts and the benefit of all of his research.

BRIAN: Well, what you just laid out, Steve, actually makes a lot of sense. And I'd love to talk about all that. You know, one of the things that interests me, I spend a lot of time, is kind of lurking in the underground. And part of the reason I do that is because I like to

know what's going on, what these guys are talking about. But you get sort of an unvarnished look at what is going on. I'll give you an example. A little while ago I was trying to - I was working on a project, actually I'm still working on this project, where I was trying to figure out, okay, what do we know about these ISPs out there that are friendly to bad guys, right, the bulletproof hosting providers, stuff like that.

Leo: Yeah, because somebody has to provide them with Internet access.

BRIAN: Right. Literally they do.

Leo: Presumably that person has some idea of the kind of traffic they're hosting.

BRIAN: Without a doubt. Well, but the problem is, is it's kind of like - it's kind of like the issue with when you find a website that's malicious or it's hosting some nasty content, and you complain to the hosting provider, and they say, well, okay, we'd like to help, but we're just a reseller. And, by the way, we're a reseller of a reseller, and you need to talk to these guys. That's kind of what happens with the bulletproof hosting stuff is they jump through a variety of hoops to cover their tracks. But I thought, well, why not just ask the people in the underground where they go to, you know, where do they trust? What are the places they go to put their sites online? And that's a kind of approach yields some really interesting results, instead of trying to go at it through the front door.

Steve: And from the things you've blogged, and this is one of the comments that I've often made about you, just from assuming, based on what you're writing, that you must have established some anonymous identities in those circles.

BRIAN: Yes. On a lot of different forums and sites. And I try not to be too obtrusive and just, like I said, lurk and occasionally interact with folks. Like I did this series, I've done a series, ongoing series on ATM skimmers. And a lot of those images and some of the videos that I got there were actually just me talking to people on these forums who were selling these devices and chatting them up and just pretending I was interested in buying them, getting them to send me more information and pictures and things and explain how the technology works. But that's about as far as I go with interacting with people on these forums, so...

Steve: Right. So mostly it's sort of passive watching. And of course you'll, by watching, you'll pick up references to other forums and URLs to other places. And so after a while you end up sort of mapping that network.

BRIAN: Yes, yes. And, yeah. As sort of a self-preservation exercise, it's usually good not to...

Steve: Keep your head down.

BRIAN: ...[indiscernible] in the forehead too much. One forum in particular, I won't name them, but they have replaced their home page right now and are redoing the site because they figured out that, not only did I get back on after the last time they kicked me off, that, you know, they had a compromise - it wasn't my fault - in the meantime. So anyway, it's...

Leo: So is it mostly IRC? Is it forums? Or is it a mix of the two?

BRIAN: Yeah. So a lot of the relationships are built on the forums, and people's reputations are built on the forums. The forums are a way for people to build their reputation as somebody who can be trusted - in a criminal way - and build a reputation as somebody who's got something to offer the rest of the community; right? So but a lot of the transacting, you know, the actual changing hands of malware, money, whatever it is, a lot of that takes place offline, you know, off the forums in private Jabber or instant message communications, stuff like that. But, yeah, the forums are sort of the open-air bazaars of the underworld, Underweb, as I like to call it.

Steve: So when you were talking about how they establish an Internet presence, like how they get websites up and so forth, what occurs to me is the issue of money because that's something in the real world which does connect us all. And on some level it would seem to be traceable. So like the old adage was, you know, "Follow the money." And I'm sure that law enforcement must recognize that that's a potential Achilles heel of any miscreants who are somehow wanting to collect money for their actions. So how does that all work?

BRIAN: Yeah, it is, well, that's a good question. So follow the money still works as a very good investigative technique. I don't care if it's journalism, if it's investigative journalism, if it's law enforcement or whatever. But there are some wrinkles; right? I mean, in the modern digital economy that we have there are lots and lots of ways that people can get paid. And, by the way, new methods of getting, transferring money are being brought online every day, and companies are tripping over themselves to add mobile payments and all kinds of other ways that you can move money around. And the really interesting thing about that is you watch the reaction of the guys in the underground because they love that stuff. The first time somebody comes out with a new way of moving money around, you can bet that there are 16 different ways that the good guys didn't think of that that could be abused. And so very quickly they hop on those.

But to your point, I mean, about following the money, yeah. Sometimes it's not that hard. They might move money from one bank account to another. But more often than not, they're moving money from one account to an intermediary, and sometimes just series of intermediaries before it gets to where - an account that they can withdraw at or use it from. And on top of that, they're relying on digital currencies, or virtual currencies or what have you. Some of the more popular ones are like WebMoney or Liberty Reserve, Pecunix, there's a whole bunch of them. But these are sort of unofficial currencies. And they can help move money around relatively anonymously. Some of them, it's not too difficult to create bogus identities and link it to regular bank accounts and push money through that way. Of course getting money into and out of these systems can be challenging, and that's really where cybercrime investigators who are following the money trail tend to focus these days.

Steve: The linkage to the real world.

Leo: Brian, if you can go to these forums, if you can get in, if you can talk to these guys, why isn't law enforcement doing this? Or are they?

BRIAN: Oh, no, I'm quite certain they are. And some of these forums are actually...

Steve: They're just not reporting it.

Leo: Yeah, but at the same time you'd think they'd be more effective in stopping all this if they were in there and talking to these guys.

Steve: It's just too vast; isn't it, Brian? I mean, it's just sprawling.

BRIAN: There are dozens and dozens of these forums. Some of the more interesting and clueful ones are in other languages, particularly Russian, and that presents its own challenges. But I think that law enforcement, I would be very surprised if law enforcement did not have a strong presence on all of the major forums out there. But being able to know what people are doing does not necessarily equate to being able to match that activity with an identity.

Leo: Right. And maybe you don't - you want to, as they did with Enigma in World War II, you don't want to bust yourself by knowing too much; right?

BRIAN: Well, right. I've found myself in situations like that before, where...

Leo: It would have to be Brian who knew this. Oh, it's that guy.

BRIAN: Well, so to give you an example, so let's say you have an account at one of these forums. It's a privileged account, and only a certain number of people can see some information. And you've got some really good information. Do you go write about it? Do you blog about it? Knowing that they're going to go back and do a full review and find out who looked at what and when and what their usage pattern is. And pretty soon that account's going to be gone. So the same thing holds true with law enforcement. I mean, anytime they decide to do something, it affects their visibility, and everybody's visibility, for that matter.

Leo: We're talking to Brian Krebs of KrebsOnSecurity.com and really one of the foremost researchers and writers about - actually, really I'd say writer first, but with all of this undercover work you're doing lately, you're really being a great source of information.

BRIAN: Oh, thank you. Thanks. Yeah, you know, the frustrating thing about these - you mentioned following the money. The frustrating thing about these alternate payment systems is the way they're being plugged into and meshed with traditional payment mechanisms. Like, you remember the - they called them the scareware, the fake antivirus stuff that pops up on your screen, you know, got this little statement...

Leo: FBI.gov. Send us, what is it, value packs? MoneyPaks?

BRIAN: Well, so it used to be you need our antivirus software. Pull out your credit

card and pay for it. But a lot of people got together and said, all right, this is ridiculous. These people can use credit cards.

Leo: Can have a merchant account.

Steve: Merchant accounts and all this. So they made it a lot harder and a lot more expensive for them to do this. And I think that's contributed to a slight shift, and that's part of what we're seeing with the ransomware is they shifted the attack a little bit. It's still sort of, we have control over your machine, you're in danger, you did something bad, you need to pay us money. But instead of asking for people to pull out their credit cards now, they're saying go down to Walmart or Walgreens or whatever and buy one of these MoneyPak or Ukash cards.

Leo: It seems so obviously dumb. I mean, obviously the FBI doesn't do this. And yet people must do it or they wouldn't continue this. There must be enough success to make it worthwhile. I mean, who's going to go to Walmart, get a MoneyPak and send it to the FBI?

BRIAN: You would be surprised. I mean...

Leo: I guess I am.

BRIAN: Look, there are a lot of people who are just joining the Interwebs every day. And maybe they aren't as savvy as some of you guys out there. But, I mean, I did a piece, an investigation, it was about, let's see, it was August of last year. And I was working with a researcher who had gotten control over a server that the bad guys were using to keep track of all the victims of their ransomware. And so it was, like every day it was incrementing, like the number of people who got infected, the number of people who - and the number of people who paid. And it was like, I think that they had, like - let me see if I can pull it up. They had - right. So you had to pay a hundred dollars to get this warning off your computer that you were looking at child porn or whatever. And you could pay a fine of a hundred dollars to avoid jail time.

Steve: To be absolved.

Leo: Now, it's $300 now, by the way. Price has gone up to get out of jail.

BRIAN: It has gone up, so true. And it hasn't been that long. So they said, you know, pay us a hundred dollars or a hundred euros. In this case it was the good guys or the white hats or - so we weren't going to use that term. But, you know, the guys who were messing with the bad guys, you know, they took over this thing. And it was an attack against a bunch of French Internet users, so it was whatever the French police is, warning on their machine. And they had something like 2,700 victims in one day. And 3.7 percent of them paid the ransom. And it was like, you

know, almost 8,000 euros in one day.

Steve: A day.

BRIAN: One day. And that's just one subset.

Leo: Who are these people? Are they organized crime? Or is it just individuals? Is it small, as it has been in the past, groups of - kind of like hacker groups of teenagers that get together? Or is it all of the above?

BRIAN: Oh, it's definitely all of the above. In the sort of Underweb space that I spent a lot of my time, I would say a tremendous amount of this is, you know, ankle-biter type, small-time cybercrime. And by this I mean, you know, these are people who may not have actually that much in the way of street smarts with cybercrime.

Steve: Skills.

BRIAN: What's that?

Steve: Skills, I was saying.

BRIAN: Skills, skills, yes, you have "nunchuck" skills, you know. Channeling Napoleon Dynamite. They don't really understand the ins and outs of doing the crime in ways that may not one day expose them to doing the time; right?

Leo: Well, I'm thinking of the guys who hacked Mat Honan, Derek the God and his - Cosmo, the guy, his friend, who's now doing jail time, or not jail time, but he's like 15, and he got caught. It was just - they were teenagers, and they were kind of ignorant.

BRIAN: Ignorant and arrogant.

Leo: And arrogant at the same time. Good combination, isn't it.

BRIAN: It's a wonderful cocktail. So it's a sure recipe for getting busted for this stuff. But anyway, these new players are joining the forums at a fairly regular clip. And they're constantly annoying the crowd, you know, the senior and established members on the forums. But they're tolerated. The senior members will put up with them because most of the top forum members, they're there because they've got different services and software for sale. And a lot of what they're selling are turnkey solutions. It's like you really don't have to know how to put up a botnet. Somebody'll do it for you.

Leo: These are script kiddies, in other words. At least we used to call them that.

BRIAN: Yeah, so a lot of them were script kiddies, and they're relying on somebody else's automation to help them get their operations up and going. And so they tend to be the biggest buyers of the services that are for sale on the forum. Now, they also tend to be the welchers and rippers of people on the forums. But nonetheless, they...

Leo: Gee, you can't trust a crook. What a thought.

Steve: And are the relationships like a piece of the action, like the seller gets a percentage of the proceeds? Or is it a one-time purchase? I'm just sort of wondering if the script kiddies end up being agents for the more senior members who are behind the scenes, pulling the strings.

BRIAN: Sure, sure. Yeah, so you asked a lot of questions there. There are a lot of things going on, particularly when somebody puts themselves in a situation where they don't - they're buying something they don't really know what it does.

Steve: Right.

BRIAN: So, for instance, for the longest time people bought phishing kits, right, to tackle phishing 20 different, you know, a little software package, and you unzip it, and you've got readymade phishing kits for 20 different things. Well, a lot of those had backdoors. And they would - the guys who sold it to you would go in and steal all your...

Steve: Aaaah.

Leo: [Laughing]

BRIAN: And that still goes on. That still goes on. And even, so some of these software, these malware services that are sold, there's no honor among thieves in the underground, really.

Steve: Right.

BRIAN: And so these guys will - some of them are quite clever, and they'll crack the encryption or crack the copy protection on these malware packages. And then they'll go and say, hey, I cracked this, here you go, download it if you want it for free. Of course a lot of times they'll backdoor it before they do that.

Leo: Wait a minute. Are you saying they DRM these? They have copy protection on them?

BRIAN: Mm-hmm, absolutely.

Leo: [Laughing]

BRIAN: They do because - and I think that that's part of the reason why we've seen a shift in the underground away from the bad guys selling software to more software as a service; right? They don't - they're not making a lot of money off that because, hey, they're vulnerable to what I just explained, you know, somebody cracks your software and open sources it or whatever, you know, or just puts it out there for any idiot to download. But what they've started to do is say, well, all right, if you want to run our software, you've got to buy a license. And this license entitles you to support. And you can file trouble tickets, and you can do all this other stuff, 24/7 support. But it only entitles you to use this - in the case of, say, a botnet creation kit, it only entitles you to use it - or an exploit kit, which is actually a better example. It only allows you to use this exploit kit at a particular domain, and your license is tied to that domain. And if you try to use it somewhere else it just won't work. And so that license allows you to do that. But that's a barebones license. And so if you want all these bells and whistles, you've got to pay extra for it. Those are add-ons. This is a la carte.

So there's a lot of that going on. And not surprisingly, one of the, I think the biggest, sort of the busiest area of criminal commerce in the Underweb is developing these plugins for malware tools that have been massively adopted. So somebody leaks the Zeus source code, as they did a couple of years ago. Well, that may have been somebody who actually had the source and leaked it against the will of the guy who created the software. Or it could have been the guy who sold the software itself. He got sick of all these people he had to support. I mean, because at some point it comes down to you have, like, thousands and thousands of users, and half of them don't even know how to, you know, they don't know anything about...

Steve: They're just clueless, yeah.

BRIAN: They're clueless, and they're constantly annoying you with questions about how to set it up and use it.

Leo: So JavaScript what is that? How does that work?

BRIAN: What's Java? How is it different from JavaScript? Where's the "any" key, you know?

Steve: Well, and of course you also have the problem that many of the vulnerabilities which these kits are designed to exploit, they ultimately get found and fixed. And sooner or later they sort of dry up across the Internet. And so something that had value initially begins to have diminishing returns.

BRIAN: Yeah. This is actually a very interesting dynamic in the underground, and it's part of the - I think it's part of the reason why we're starting to see a subtle shift in the way a lot of these exploit kits are sold. Are you guys - do you think your readers are familiar with what we're talking about here?

Steve: Oh, yeah, for sure.

BRIAN: Okay. And so typically when a new vulnerability comes out, like if you read on a blog somewhere like, I don't know, KrebsOnSecurity.com, you might see a notice about a zero-day vulnerability in Java or something. In short order, that will be in all of the

exploit kits. Okay? They're very quick.

Leo: Short-order - a day, two days, a week, a month?

BRIAN: Day or less.

Leo: They're fast.

BRIAN: Yeah, because it's...

Steve: Because it's all about the window of opportunity.

Leo: Right, because as soon as people start patching, you're out of luck.

BRIAN: Well, it's not just that. Their customers, again, they're answering to their customers.

Leo: This is our business.

Steve: Right.

BRIAN: Yeah, this guy over here is selling...

Steve: Their customers want the latest vulnerabilities in their kits.

Leo: So they stay up late that night and...

BRIAN: They're just like the rest of us.

Leo: ...write code.

BRIAN: They want the neatest iPhone and, you know. So, yeah, they'll come to these guys and say, hey, you know, Joe Schmoe has this exploit in his pack. How come you don't have it? And so...

Leo: Oy. How many of these are there? And is it, I mean, we talk about Metasploit Framework a lot, and that's kind of on the other side of it. But it's similar to that; right?

BRIAN: So how many exploit kits are there?

Leo: Yeah, how many kits are there? And where do you get them? You just go online, and there are websites, right, that sell these?

BRIAN: Yes. Some of them have just regular websites. There's one right now, I'm thinking it's called stxyx-crypt dot maybe ru. But, yeah, you can go and just sign up and plonk down some money, and you'll get a license, and then they'll send - they'll sell you, you know, ancillary services. But there are, to answer your question, there are dozens of exploit kits. And there are lots that have sort of kind of been thrown out there and, hey guys, check out my kit, play with it, let me know what you think, and then some of them, you know, the community just takes a crap on, you know.

Steve: Pooh-poohs it, yeah.

BRIAN: This sucks, you know, go back to...

Leo: [Indiscernible] school.

Steve: Go get a day job.

Leo: Is this it? Styx-crypt, a well of wishes awaits you in the crypt of decay?

BRIAN: No, I don't think so.

Leo: I like that one, though. It's got Russian on it.

BRIAN: Yeah. Let me...

Leo: I don't know if I should go there. They're selling innovative and world-leading obfuscation of JavaScript.

BRIAN: Oh, that might...

Leo: It looks legit, but then, if you kind of - it's kind of like HTML morphing FUD. FUD morphing.

BRIAN: Yeah, so you are on the Russian version or the...

Leo: I'm on the English language. Should I go to the Russian version? Would I get more interesting things?

BRIAN: No, you just - yeah, styx-crypt.com.

Leo: Yeah, that's it. So it doesn't look like a malware kit site.

BRIAN: Well, did you miss that part in the banner that says Styx Sploit Pack?

Leo: Oh, okay. The Styx Sploit Pack. Let's take a look. Gentlemen, it's time to announce the next-generation product for your viewing pleasure, the Vulnerability Browser Stress Test Platform.

BRIAN: Right.

Leo: They use GIT [laughing]. They update from GIT.

BRIAN: This is really - I absolutely love this phrase, this turn of phrase, "stress test," because people are going to buy this so that they can stress test their product.

Steve: Other people's browsers.

Leo: I love it that you can update it via GIT twice a day.

BRIAN: So here's another script kiddie-type activity that's gone off the hook over the last couple of years. It used to be very common that the script kiddies would go - this is where they got their name from. They would go grab some script that allowed them to hack into a website. And it's really just like an SQL injection or something like that. And you can still do that, right, like there are sites you can go that are called "Google dorks." And you just Google "Google dorks," and you'll see it. But they're basically strings that you can - search strings you can put into Google, and they'll bring up a listing of websites that are running outdated and vulnerable versions of software that can be exploited so that you can deface the site or add malware to it or whatever. So it used to be - and this still goes on to some degree. But it's not - it's a lot less innocent than it used to be. Used to be, like, yo, man, hey, you know, Hacker G was here, right? And that was pretty much it. And they'd do it to all the sites that they could find that were vulnerable and lead to...

Steve: Not it's the iPhone SDK site that infects Apple and Twitter and Facebook.

BRIAN: Well, no, just I was - this is a long way of getting to the stress testing thing because what they do now is they leave behind a little - a shell. And it just allows them - it's a backdoor that allows them to get back into the site. And in almost every case the shells include a booter component. And all that does is it allows the hacker to use that website, that server power, in denial of service attacks. And so it's not real hard to build a botnet of hacked websites to use in DDoS attacks this way. You just find a bunch of sites that are vulnerable, you upload your booter shell, and you're good to go. I wrote a story about a guy that was offering a booter shell service, and this was, like, last year. And it was pretty clearly being used to knock people and different things offline. And he got really upset with me, and he's like, oh, no, this is just stress testing, and it says that in the Terms of Service, this is stress testing, so - it's just stress testing.

Leo: Yeah, no, it's okay. If you use this for illegal purposes, it's on you, man.

BRIAN: Well, I think, you know, this is kind of a debate that is raging right now, which is, is the sale of software vulnerabilities, like if you find a new vulnerability in Java, and you're selling it to the highest bidder, are you breaking the law? Most people, at least in this country, would say no, not by today's standards, not by the way the law is set up. And a lot of people are saying, well, do we need to change the law? Personally I don't think it would change the dynamic or the reality at all, but...

Steve: The behavior, right.

BRIAN: Right. It wouldn't change the market, I don't think. And if anything, it would make these things more valuable.

Steve: So it sounds like your focus, because of like the access to this community, is sort of the demographic that you've been sharing with us. Do you see the presence of organized crime here? I mean, we hear stories. I've had FBI guys tell me that they really see, like, organized crime recognizing that there is a potential to make money through this kind of Internet chicanery.

BRIAN: Oh, it's everywhere, yeah. There are a lot of people use that term, "organized crime," and it's probably more apt to call it "disorganized crime." Even the guys who are very good at what they do and have been doing this for quite some time, a lot of them are, I think, best thought of as more like independent contractors who work together from time to time when it suits their purpose, and everybody's happy about it.

Steve: So it's just sort of the social - it's sort of the nature of the people who are doing this is that they're loners, and they're in their parents' basement or whatever. I mean, they're just - it's not the kind of thing that you have old-school family organized crime doing.

BRIAN: I wouldn't say - so it works both ways; right? I mean, there are, just like you and I are talking remotely, I don't think we've met face to face, this is a lot of the guys in the cybercrime community. They don't want to meet face to face. They want that distance.

Steve: Yeah, you and I are using our real names.

BRIAN: Right. But they'll find each other on the forums. And what you tend to see is it sounds like an exaggeration, but it isn't really unlike something you would see in, say, "Ocean's Eleven," right, where you have one guy who's really good at writing malicious software that steals banking information. And then you have another guy who's very good at writing custom web injects for specific things. And then you've got another guy who specializes in procuring domains that won't get shut down very quickly, website hosting that won't get shut down. Maybe he even runs all of the services. So it's very common to see groups perpetrating criminal conspiracies.

Steve: Combining their various talents.

BRIAN: Right, combining their various talents. And the Justice Department did a really interesting series of indictments and arrests. One guy was, I think, in Rumania. The other was Russian, but had come to the United States. And then the other guy I think was in Moldova. But it was that same kind of thing. One guy was in charge of bulletproof

hosting. One guy was in charge of authoring the malware. And the other guy was developing custom web injects. And that very, I mean, I think that meets, for most people, that meets the threshold of organized crime because, if it works for them, they'll keep doing it. And that's something I've been really spending a lot of time focusing and writing on, and that is the cyber heist against the small to mid-size businesses out there. And I would be remiss if I didn't mention that because it is something I spend a lot of time researching and writing about.

And I do so because I feel very passionately about this. I talk to - I travel a lot. I talk to small business owners all the time, just, you know, chat them up. And I always ask them, I say, well, hey, do you bank online? Do you know how exposed you are? Do you know if you get robbed, that's gone, that money's gone? The bank doesn't have to put it back? People don't know that. And they don't know that this can happen, their business can be ruined because they got a virus infection on their machine. And but unfortunately we're seeing that over and over again every week.

And so I would characterize those as organized crime attacks because they require certain resources. And they have to hire people to hire the money mules, the people that abscond with the victim's loot and help the bad guys launder it. They have to hire foreign money mules and people over there in their own countries to be intermediaries, as well. There's a lot of organization there and orchestration that has to go right for them to get paid. So that in my book is organized crime. And there's a lot of that going on.

Steve: And so I guess in general, as we've seen the evolution of this over the last decade, it's switched from script kiddies running little botnets to blast each other off of IRC servers to, I mean, real money-making enterprise. The point is now not just to, as you said, post your name on, like do a website defacement for its own sake, but to actively somehow turn some advantage for the person who's doing the exploiting.

BRIAN: Yeah, there's no question. And in some ways, you know, I think part of the problem that we have with some of the more advanced attackers, so when an organization gets popped and they lose all their customer data, or a company, a Fortune 1000 company gets infiltrated by foreign cyber spies, and five years' worth and billions of dollars worth of R&D gets siphoned overnight, I think those are all cases where the bad guys have identified the valuable stuff, much more directly, much more - they're thinking about it a lot differently than the folks who are getting breached. And I think that that mindset is changing from the organization side.

Steve: Right.

BRIAN: People are really, organizations are really starting to wake up to the fact that it's really not hard to get breached these days. And the focus needs to be on just accept, you can't keep the bad stuff and the bad guys out. They're going to get in. And, you know, the financial institutions figured this out years ago, and they said, well, we only have so many resources. We can't spend infinite amount on defense; right? At the end of the day, the banks are the best bean counters in the world. They know what it's worth and what's at risk.

But by the same token, they've looked at it and said, hey, we've got scarce resources here. How do we best spend our money? And they decided, well, let's make sure, let's make damn sure we know, when we get breached, that we know very quickly we got breached, and we can respond and take care of that before it becomes a much bigger problem. So I think, unfortunately, a lot of the stuff we're seeing with the espionage attackers breaking into companies is an artifact of...

Steve: Oh, the companies being more aware now than they used to be.

BRIAN: It's an artifact; but, I mean, a lot of the defenses the companies have in place are built to defend against attacks that were very - were more prevalent years ago. They're not necessarily built to defend against today's attackers. We still sort of rely on some of these things that are supposed to provide protection, but provide diminishing protection every day, of course stuff like antivirus and things like that. So all I'm saying is it requires a mind shift, a different mindset when you're thinking about these attackers, to one of containment and response, rapid response. And you know how these things kind of shift. They kind of swing back and forth like a pendulum. It's like, is it thin client, or is it servers on the LAN? Is it cloud? Is it, you know, whatever. Seems like we go back and forth.

But for a while there it was like, oh, let's just automate everything. We can't handle all these logs. We can't look at - we can't possibly look at all this information we're collecting about what's going on in our networks. Let's automate it, and then we'll know what's going on. Well, yeah, okay, but only if somebody's really paying attention to the reports that those things are spitting out. And so...

Steve: We had that perfect story a few weeks ago that the Verizon security blog brought to light where one of their clients was looking at their logs and discovered that there was a VPN connection to China that had been going for many months, and they thought, oh, my god, we've been hacked. And it turns out that it was one of their own employees had subcontracted his own job out to a Chinese company, and they were actually doing the work for him.

BRIAN: I want to give that guy a genius grant. I mean, come on, you know, I mean, like, how many other people could have done that same thing, and probably still could.

Steve: And pulled it off, yeah. He was just sitting there in his cubicle, surfing eBay and updating his Facebook page.

BRIAN: And watching cat videos, I think it was.

Steve: And getting top ratings from his employee evaluations, saying, oh, this guy is just great. Look at the fantastic, well-commented code that he's creating.

BRIAN: Yeah, yeah. So I guess what I was saying there is - go ahead.

Steve: Go ahead.

BRIAN: No, I was just saying, with automation, I think we're starting to swing back now. People are saying automation is great, but let's step back from it a little bit and try to put some more humans in the loop and really have people actually looking at this stuff. And the Verizon thing you mentioned is actually very apropos here because they do an annual breach investigations report which I always recommend people read because they just - it's just got a tremendous amount of useful information for anybody who's involved in defending networks. But basically they said one thing they saw over and over again with these breaches when they responded to companies that had breaches, they said that the evidence for the break-in was there. It was there in the logs. And if anybody had bothered to look, even - not even, like, reading the logs. They didn't have to read the logs. All they said was it would have been enough for them to, like, scroll through very fast the logs, and the anomalies jumped out.

Steve: They would see - a big block of something would just stand out, yeah.

BRIAN: Right. So I thought that was really interesting.

Steve: In the dialogue in the underground, do you see people talking about, discussing, or bragging about actual money that they're making from these exploits, where they're saying, hey, I used this exploit kit, and it's generating this much revenue for me? Do they discuss that openly?

BRIAN: Not so much, I mean, what you tend to see is people will post screenshots of, say, their Blackhole exploit kit administration panel showing that, of the hundred thousand people who went to their redirection sites that pushed them toward the malware, 10 percent of them were served an exploit. And so they'll brag about that. And you can make some inferences about how much money that could bring them, depending on what sort of like affiliate programs they were signed up with and stuff like that.

Steve: [Laughing]

BRIAN: Because, again, it comes down to, you know, a lot of these guys, if they sign up for one of these pay-per-install programs, they don't know what they're installing. They're getting paid to push some installer program. They don't really know. You know, it could be something that takes over their botnet, I mean, as far as they know. But they're getting paid for every install.

Steve: So from all of this, from your perspective, and now looking at our audience of end users, if you could offer advice to individuals about how to keep from being victims of this, how would you sum that up? What would you suggest?

BRIAN: Yeah, I guess I would just say a couple of things, and I hope you don't mind me pointing people to some resources on my site because...

Steve: No, no, no, no.

BRIAN: ...I could just spend all day talking about this, as you can see. There are two resources on the right side of my blog, KrebsOnSecurity.com. One is a graphic, "Tools for a Safer PC." And there's just a whole bunch of tips for people. It doesn't matter if you're running a Mac or Windows or whatever. There are a lot of tips there that can help people...

Steve: Where you've pulled everything together into a nice organized list.

BRIAN: Tried to put a bunch of stuff together that, if you follow these tips religiously, you're probably not going to run into any problems. A lot of the stuff you're going to run into is sort of picking the low-hanging fruit and taking advantage of the fact that, for better or worse, it does require some amount of vigilance to keep up with this stuff. And if you fall behind, that's when it becomes a problem. So at the very least, gosh, I tell people to grab one of the tools that helps them stay abreast of the latest security updates for third-party software. So, like, Secunia's Personal Software Inspector is a really good one. It's free. Same with File Hippo's file checker, Update Checker. Both of them, really good in letting you know about new stuff. That's real important.

And as I try - and there's another resource on there, on the right side of the site, that I built to really try to drive home the point that, look, this isn't personal. If you get hacked, it's not because the bad guys are interested in you or your chats with Sally or Suzie Q.

They're after your computer. They're after the resources that your computer offers them. And that may include your banking information. But part of the reason - so the graphic I'm referring to is called the Scrap Value of a Hacked PC. And this thing is actually in the process of being translated into, like, 17 different languages at the moment.

But what I wanted to do with this graphic was to explain to the person who says, "Well, I don't bank online. I don't have sensitive information on my machine. I don't see why it should matter if I keep up with this stuff." And this graphic tries to explain to people, okay, well, here are 59 different ways that it can impact you, and your system can be reused by cybercriminals. So I think anybody who spends any time just looking at this hopefully shifts their mindset a little bit to being more proactive about that stuff because it's a heck of a lot easier to keep your computer from getting infected than it is to actually get it uninfected once it's messed up.

Steve: And in fact these days the malware is so pernicious and digs itself so deeply into one's system that it's arguably - it's either impossible to get rid of it, or certainly impossible to ever know that you've really gotten rid of it because we keep hearing stories about people who, like, really understand their machines and have removed every trace of everything that they can find, and a couple days later, whoop, the thing comes back, like from some dark corner where it was hiding somewhere.

BRIAN: Yeah. I always tell people, spend some time on some of these PC help forums and watch the experts go round and round with these guys and, oh, yeah, you're clean, and they come back a couple days later, and, wham, they're not. Yeah, I mean, that's an excellent point. Ah, shoot, I lost my train of thought. I was going to tell you about another tool.

Steve: What I was going to say was that I think one of the best pieces of advice I got from you and your site, and it's something that I have credited you with and echoed it whenever it occurs to me, and it's just, it's so simple and pithy and perfect. And that is, if you did not go in search of some software, do not install it.

BRIAN: Yeah.

Steve: The idea being - go ahead.

BRIAN: No, that's actually, that's absolutely right. So that's part of my three rules. If you didn't go looking for it...

Steve: Yup, I thought I remembered that there were three, yup.

BRIAN: If you didn't go looking for it, don't install it. If you install it, then...

Steve: Yeah, because so often, yeah, because so often we're being offered something as a consequence of some action. And it's like, oh, you don't have the latest version of Flash. Click here to download the latest version. It's like, oh, wait a minute. If you didn't go to Adobe to go get Flash, don't do it by having it offered to you.

BRIAN: That's exactly right. And that's traditionally been a huge vector for malicious software. And that's actually, the Tools for a Safer PC, that's at the very top. There's a link to the three rules. So basically, yeah. If you didn't go looking for it, don't install it. If you need to install it, get it from the source, don't get it from a third-party wherever possible. And if you installed it, update it, right, no-brainer. And if you don't need it, get rid of it because then you don't have to update it, and you don't have to worry about it.

And it decreases the attack surface on your system.

So these are really - where I was going before with the point I forgot, the reason I say it's - I emphasize prevention as opposed to cleaning up after the fact is I think that where we're headed with a lot of this - so right now the big scourge out there is, for your average consumer, is this ransomware stuff we talked about; right? But by and large that ransomware still is not very common where it encrypts your files. There was a spell where that was going on. It was mostly attacking people in Eastern Europe and Europe where they would get on your machine, and they'd encrypt all of your data, all of your documents, everything you hold dear, your photos, whatever, with very strong encryption. And you didn't get your files back unless you paid the ransom. I don't know why...

Steve: Which is brilliant because it's better than wiping out your computer or deleting them, which doesn't give them any value. This is a way of saying, hey, if you want this stuff back, then you've got to pay us. It's, unfortunately, it's evil genius. It's brilliant.

BRIAN: Right. And it's going to get even more evil genius, I think. And I think we're going to see a resurgence of these attacks at some point. And think of it this way. I try not to talk about these things because I hate to give the bad guys ideas. But then I remember they already have these ideas, so they're not getting it from me. But encrypting files, imagine. You've got something that encrypted your files with 2048-bit encryption, good luck. You're going to pay that ransom if you want those files, or if you don't have them backed up. But guess what. It's really not that difficult for the bad guys' ransomware to go and look to see what network drives are on your system and then go encrypt all of those files, as well. So maybe you backed up your files, so you're thinking, oh, screw these guys, I'm not paying my money. And then you go and look and, wait a minute, we have a problem here.

Steve: All of your Dropbox files are encrypted also.

Leo: [Laughing] Right.

BRIAN: Yeah. So, scary stuff.

Steve: Well, Brian, this has been perfect. It's exactly what I was hoping you would bring to the podcast, and you've been great. So thank you very much.

BRIAN: Well, thank you.

Steve: I mean, I talk about you and your site all the time, so I'm glad that you gave it some plugs. I absolutely want our listeners to go to KrebsOnSecurity.com and check out your resources, too.

BRIAN: Well, thank you very much for having me on. I really appreciate it.

Steve: And is Leo there anywhere?

Leo: I'm here, yeah, yeah, yeah.

BRIAN: Hey, Leo.

Leo: And I'm going to start recommending people go visit that section on, you know, it's called "Tools for a Safer PC," because I think this is really great stuff.

Steve: Yeah.

Leo: And he recommends, Steve, NoScript and all the stuff we talk about all the time.

Steve: Perfect.

Leo: Yeah. Thank you, Brian.

BRIAN: Well, thank you. I'm getting some nice traffic from your TWiT.tv thing.

Leo: Good. Lot of people going there, yeah. Including me. Brian Krebs. We're going to take a break. And, Steve, you have security news; right? Back we go to Steve Gibson. And we're a little upside down because Brian was on, so we're going to do the security news now, Steve.

Steve: Well, yeah. The big news of the week, I mean, and this was news that made it to all of the mainstream network news coverage, of course, is this Mandiant report that came out. Their acronym for a bad actor on the Internet was "APT1," they called it. And we know APT is an acronym for Advanced Persistent Threat. That's the technology or the name that's now been given to those, you know, the whole concept of a network being penetrated and the bad guys essentially establishing a beachhead there that we first, I think, encountered that acronym in the RSA, that infamous RSA break-in where all of the keys got exported from RSA. Well, this Mandiant organization - I tweeted a bunch of links just before the podcast, so if you check my Twitter stream at SGgrc, you can find them. It's a long report [bit.ly/WR2dvJ] where they lay out the basis for their conclusion that this is Chinese military, the PLA Unit - they have a number - 61398. And they've got satellite reconnaissance photos of the building where this is being done once upon a time, some years back, and then it's been all renovated, and it's all shiny, you know, more recently.

And apparently this is the - they've, over the course of time, they've tracked down more than a hundred attacks against U.S. interests, typically business interests in the United States, which they're alleging was formally authorized and perpetrated by the Chinese military. Now, there is an interesting rebuttal to this. I think I also posted that. I'm not sure that I did. But in all of this, it's easy to get a little hyperventilated from this. I mean, I saw it on the news yesterday. Everyone was talking about it on several of the different programs that I was watching. Yes, the Chinese Army is spying on you, they were saying.

But the SANS security newsletter had what I think is probably the best sort of, okay, push back from your computer and take a deep breath and what does this really mean. And so paraphrasing from what they wrote, they said: "In the last 24 hours, most major news outlets highlighted Chinese military and military-related hacking of American companies. BusinessWeek's cover this week, in big letters: 'Yes, the Chinese Army Is Spying on You.' Mandiant provided strong documentation. It's a big story."

And then SANS asks: "But is it the right story? If you know that the People's Liberation Army is spying on you, do you change your defense? If so, how? Do you look for Chinese language intrusion prevention tools? The continuous China bashing simply reflects the inability of watchers to see evidence of the stealthier attacks made by other nations that may take a different approach to penetrating our telecommunications and banking and power systems and stealing our national wealth."

Leo: Well, in particular, you know that we were talking about the Apple/Facebook/Twitter hacking, and the presumption was, oh, it's Chinese hackers. No.

Steve: No.

Leo: It was from Eastern Europe, as far as we could tell.

Steve: Yes. And so, and that's the point I think that is very good. SANS goes on, saying: "The number of bad actors, spread across nations, terrorists, anarchists and criminals, is so great that their identity is not as important as what we do to defend our systems."

Leo: Yes, yes. You might as well assume - you always called it "Internet Background Radiation."

Steve: Yes, IBR.

Leo: It's more aggressive, and it's more effective than ever before. But it's not relevant to worry about where it's coming from. Much more important, what do you do?

Steve: Yes. I think that's the point is that, yeah, you can get all worked up about the nature, or like the direction a threat's coming from. But the point is what you're really concerned about is protecting your homestead.

Leo: Well, it's the only effective thing. I mean, you might say, it might be fun to saber-rattle and shake your fist and say we're a superpower, how dare you? But really that's not going to be as effective as simply doing your best to lock things down. The question is, Steve, and Brian kind of alluded to this, the banks just gave up: Is it possible to lock it down?

Steve: Well, and what SANS says that I think is the key here is they where they said "The number of bad actors spread among nations, terrorists, anarchists, and criminals is so great," SANS says, "their identity is not as important as what we do to defend our systems because they exploit the same weaknesses."

Leo: So one fix covers all.

Steve: Yes. So he says, or SANS says, "The most important answer to what we should do was released last week in a White House, DHS (Department of Homeland Security), NIST meeting. The defenses specified in that paper, written by CSIS's Jim Lewis [bit.ly/WR2IG8], block the vast majority of the Chinese and other attacks. What we as a community must do is identify the barriers that stop broad-based adoption of these defenses and lower those barriers."

So what I thought was so interesting, and this I definitely, I linked the PDF, CSIS is the Center for Strategic and International Studies. They produced a report, it's not long, I think it's, like, 11 or 12 pages, a PDF that was assembled by Australia's Defense Signals Directorate. Australia's DSD is a little bit like our NSA. And in fact they combined this with NSA research that identified three policies that would consistently reduce risk by 85 percent and often to zero.

So the first of those is use whitelisting. Allow only preauthorized software to run. And that's something we've talked about before. It is difficult to do practically, but we're beginning to see it. I mean, arguably that's what Apple's curated store is, is to some degree a whitelisting protocol where they preauthorize software that they will allow their iOS devices to download. And of course we're also seeing that now in the Mac store, and also in some of the Android stores. So but in a corporate setting you can imagine IT finally saying, okay, look, we're locking these things down, period. You get to use this, this, this, and this. And your OS, by policy, simply will not execute anything else. So, again, it's draconian. But ultimately it's what you have to do in order not to run stuff that might be bad.

And then, No. 2, very rapid patching of both operating systems and programs. And so this is a recognition of the fact, as we were talking with Brian, that there's a window. And Brian made it very clear, you know, he saw the actual dialogue, has seen the actual dialogue going on in forums where somebody says, hey, their exploit kit now has support for this new vulnerability. When are we going to get it on ours? So, I mean, and it's a matter of overnight that suddenly the exploit kits are updated because there's a window of opportunity. So that means that we want to close that window on the receiving end as quickly as possible. So very rapid patching is the other thing that is very important. I mean, how often are we talking about people getting exploited on vulnerabilities that have been known for months? So if the vulnerability - well, I'm sorry, and the patches, the fixes have been available for months, that the systems are still being compromised that way, then that tells you they're not being patched with any kind of schedule. So that becomes very important.

And the third principle is minimize the number of people who have administrative privilege. And of course we understand what that means. If malware gets to a machine and is trying to impersonate that user, but the user cannot do much on the network, then it can't, either. And so that's crucial for minimizing the attack surface against your network.

And then they had some interesting statistics in this report. They said that, under the

banner of "Hacking Is Not That Hard" - I thought this was - this is some of the most interesting stuff we've seen, and not surprising. They said more than 90 percent of successful breaches required only the most basic techniques. Only 3 percent of breaches were unavoidable without difficult or expensive actions. Outsiders were responsible for most breaches, not, as we have sometimes been led to believe, insiders, although certainly insiders have been, historically, have created problems. 85 percent of breaches took months to be discovered. The average time is five months. 96 percent of successful breaches could have been avoided if the victim had put in place simple or intermediate controls. 96 percent.

So what we're seeing is that the breaches that are now occurring are not hard to conduct, and they are essentially against corporations and entities with no protection. They're just, they're running an old version of IE. They're, I mean, they're just - they're clueless companies that are just not looking at this at all. Their business is not computers. They use their computers because everyone has to have, you know, computers.

Leo: But, Steve, when developers at Apple get hacked, presumably these guys know what they're doing, and Apple's got to have very good corporate security. They're paranoid as hell. And they still get hacked internally?

Steve: Well, and this was...

Leo: They ain't using IE5 at Apple.

Steve: Right. It was, in this case, it was a Java exploit. And they visited a compromised site; iPhoneDev SDK site was hacked to plant the exploit. And so some Apple developers went there, got their machines exploited. Now, what's interesting is that Apple's response to this was, well, yes, but new Mac OS X doesn't have Java, and it gets turned off after 35 days of non-use, so...

Leo: And the browser Safari tells you, are you sure you want to run Java? But obviously these developers were using Java. Maybe it was part of their job. They needed to - maybe they were writing stuff in Java. I don't know. Maybe they were writing Java browser plugins, for all we know.

Steve: Leo, Java is the No. 1 language.

Leo: Exactly.

Steve: So, I mean, you're going to have Java around. You just don't want - you want it in your computer and not on your browser unless you have to have it.

Leo: And I suspect that these developers did. And I also believe, you know, Apple, apparently, even though Apple is the last we've heard about, was the first to

discover this. And I'm betting that Apple and Facebook both have very stringent security procedures and detected this immediately and remediated it immediately, I would guess.

Steve: Yes, yes.

Leo: I mean, we don't know, but...

Steve: And this was your typical corporate breach. Bloomberg carried a story from two unnamed people who were, quote, "familiar with the matter," unquote, told Bloomberg that the hackers appeared to be looking for research, intellectual property, or other private information that they could sell...

Leo: It's industrial espionage now.

Steve: Yeah, exactly, it's espionage that they can sell on the underground market.

Leo: Industrial, not cyberwarfare. It's industrial espionage.

Steve: Right, right.

Leo: Economic espionage.

Steve: Just as we were launching the podcast, Adobe released their emergency Reader patch [t.co/aKSJKrBt]. We spoke about this last week. Remember that there was a very bad exploit that affected versions 9, 10, and 11 that was in the wild. It was being used for targeted phishing attacks. There was no known defense, as long as you were using Adobe Reader to open PDFs. It's funny because, whenever I tweet this, I get feedback from Twitter saying, "Who uses Reader?" It's like, okay, I know.

Leo: Our audience doesn't, but everybody in the world does.

Steve: Yes.

Leo: And it comes with many computers. And, I mean...

Steve: Yes, and many sites where you go to, like, download a PDF, it says, oh, if you can't read this...

Leo: Download Reader, yes.

Steve: ...click here to download Reader.

Leo: I was looking at a firmware update just last night, and it said "Download Reader first." And you know what, it's a firmware update. I actually don't need to download Reader for it. I guess that's for the manual. And I sure as hell am not downloading Reader. And, geez.

Steve: Anyway, so for anybody - but we also know that the reason Reader is insecure is it is so bloated and so big and it has JavaScript in it and it loads and runs plugins and does all this other stuff for you. In some cases people have to have it. So if you're in a corporation where Reader is the only thing that works for you, Adobe's Reader, then you should know, just go to www.adobe.com/downloads/updates, and that will take you to a page. You select Adobe Reader, and then you've got a choice of Windows, Mac, and Linux. Choose your platform and get the update. It's dated today, February 20th, and you definitely want to do it because these things were bad, and they got fixed quickly.

Also in update land, Firefox 19 was just released. And so I clicked on the Help menu, and I saw the little update button. I was on 18.0.2, you know, from yesterday. And now we're at 19. So I said, yes, update me. And it closed Firefox, and it opened again, and what was interesting was that I was using the Sumatra PDF plugin. That's one that I had been using for viewing PDFs in Firefox. And as we've been expecting, it was with version 19 that Mozilla finally put their viewer front and center for PDFs. So the PDFs tabs that I already had open now open with the built-in browser PDF viewer. And it looks very nice. I don't have much experience with it because it's only a few hours old. I did see some people tweeting that it's been working for them since they started using it. I think they adopted it earlier. It was available I think back on 17, but it wasn't automatically taking over.

And interestingly, I get a little attention bar at the top saying, sort of, I think, because they're still sort of sticking their feet, their toes in the water here, they said, "If this page doesn't render correctly, click here to render with an alternative." So they know that they replaced a plugin that I already had. And I'm happy because I'd rather - as long as they're not going to have any security problems. I suppose we'll know here before long. Hopefully they've done this very carefully; but as we've seen, careful doesn't always cut it. Sometimes you need more than that. But anyway, so Firefox 19 has a native PDF viewer. Just shut it down or go into the Help menu, fire up Firefox again, and you should have it. And the viewer looks very nice.

I just thought I'd give an update on GRC's Universal Plug & Play test. When I checked this morning, we were up to 2,290 discrete IPs have been found.

Leo: That's, like, twice what it was last week. Wow.

Steve: Yes, yes. Although I think it's slowing down.

Leo: These are routers that are vulnerable to the UPnP flaw.

Steve: Correct. Well, actually it's routers that...

Leo: That responded to your probe.

Steve: Yes, that may be vulnerable, but definitely have the Universal Plug & Play publicly present. And that they should not have, absolutely. In the ongoing quest for the best UPnP acronym, we have a new submission from someone on Twitter for UPnP, is Ur Probably Now Pwned.

Leo: [Laughing] I like it.

Steve: I think that's the best one so far.

Leo: That's very good.

Steve: Ur Probably Now Pwned. And here is a great page, Leo. You're going to like this. I created a bit.ly link for it, so it's verbal: bit.ly/xorxor, all lower case. What I like about this is I've often talked about how perfect XOR is for encrypting something. And remember that XOR isn't particularly amazing. I mean, it's a simple concept. If you XOR zero with something, you get the something.

Leo: Wow. This is really - so they've got a picture of Charles Babbage. And they AND, OR, and XOR it.

Steve: Yes.

Leo: Wow.

Steve: And isn't that, I mean, I like this because it is so clear. It just says - so what they did was they took pseudorandom noise, and they XORed the noise with the picture, or they ORed the noise with the picture, or they ANDed the noise with the picture. Now, so the AND and the OR are interesting because they're alternative logical operations. What's compelling, though, I mean, I get why, if you XOR noise with something, none of the something remains. But that's the key. That's why, if you just take a good source of a pseudorandom bit string, and you XOR it with plaintext, what you get is noise. It's just, it's almost counterintuitive. It's like, wait a minute, why does nothing of the original survive? But this makes it very clear that all you get is noise. So this is sort of a graphic visual demonstration: bit.ly/xorxor.

Leo: Now, we don't use XOR because it's reversible; right?

Steve: No, no, we do.

Leo: We do.

Steve: Yeah, yeah. And that's...

Leo: But it is reversible.

Steve: That's the beauty.

Leo: If you XOR it again, you get the plaintext.

Steve: Precisely. So if you took that picture of absolute noise, and you XORed it with the original stream of bits, then it comes right back. And that's the original RC4-style encryption, RC4 that was used in the earlier WiFi. It was mis-implemented so that it didn't - the RC4 cipher works by sort of stirring up a bunch of bits in a pot. And there are weak keys that don't initialize the stirring very well. And even so, the initial stirring, if you start using the bits immediately, they're not very well scrambled. But if you simply stir it a while, then you start using it. Even though it's a simple algorithm, it produces a very good pseudorandom bitstream based on a key. And that's what WiFi was using, and even WPA2 can use that. It doesn't have to be using AES. It can be using RC4. And it's very secure when it's used properly. And so this just demonstrates that something as simple as an XOR, where you simply conditionally invert the bits, it ends up with nothing surviving of the original.

Okay. Now, this is the most bizarre, random thing I've ever said, which really is saying a lot.

Leo: That is saying a lot. Yes?

Steve: I saw - I was watching some video of some guy taking apart a PC. And it was like, we're going to, I don't know what it was, add 12 video, you know, graphics adapters to your machine or something. And the point was he was putting the system back together, and he used a power screwdriver to put the screws into the back of the case. And I just - it just made me cringe because - and the guy lost all credibility with me, frankly.

Leo: Wait a minute. Because he was using a power screwdriver?

Steve: Yes, to put the screw in. You can use a power screwdriver to pull the screw out. That's fine.

Leo: Okay.

Steve: The point is, and this is something that my grandfather taught me when I was, like, five, and I've never forgotten it, and it's just a little piece of wisdom that is so cool. And that is, any time you - and this is why this is extremely random. But, you know, what the heck. Any time you are screwing something in, first back it out. Put a little pressure on the screw...

Leo: Oh, because you could strip it so easily.

Steve: Yes.

Leo: Yeah. I've done that so many times.

Steve: Put a little pressure on the screw and turn counterclockwise. You will feel it go click. And so that...

Leo: Yeah, as it falls into the thread, yeah.

Steve: Yes. And so that, I mean, wood screws, metal screws, doesn't matter. Just back it out, and it'll click. Then you can then go forward. And if you have to use a power screwdriver, fine. But get it started.

Leo: But you're worried - what you're saying is it's so easy to strip a thread with a power screwdriver because you don't feel it. And if you're not in the thread, it'll just make a new thread.

Steve: Exactly.

Leo: Yeah, yeah. That's a very good point. It's very easy to do, yeah.

Steve: Well, and if you've got a power screwdriver, it's got all this torque there.

Leo: Right, you don't need...

Steve: It just goes [angry whirring sound]. And before you know it you've created a round hole with no threads.

Leo: I did that the other day. I was opening a MacBook Air, and they have this

Pentalobe screw - I'm not using a power screwdriver either way - Pentalobe screwdriver and the world's tiniest little screws. And it's very easy to miss the thread. Even if you do back it out, it's very hard. And once you get it screwed up, it's never going to go in right.

Steve: No, that's exactly right. So it may be something that everyone goes, yeah, yeah, Gibson, we know about that. But if it's not something you've ever heard before, next time you encounter a screw, just think about it. Just...

Leo: So you never use power tools to screw in.

Steve: No.

Leo: Only to screw out.

Steve: Yeah.

Leo: That's actually a very good point. I never really thought of that. I have used power screwdrivers because I'm lazy.

Steve: Also, Leo, you can't - you have also no feedback on tightness. I mean, anyone who's a craftsman, you'll tighten it down, and then you'll give it just, I mean, just enough, like when you're mounting hard drives. You want them to be, like, firm, but you don't want to, like, torque the whole hard drive frame because you just bear down on the screw so much. So it's like, no, just, you know, enjoy the process of putting the screw back in.

Leo: Enjoy the proc- enjoy what you're doing.

Steve: Yeah. You know, take some pride in having your threads well meshed. That's all I'm saying.

Leo: [Laughing] You know, it's funny, I never thought about that. But I do know what you're - the cross thread, I know what you're talking about. That happens to me all the time.

Steve: Yeah, and if you just - it's very satisfying. When you just go backwards, it kind of goes click, and you just, oh, it's like, oh, okay, there we go. Then we just go smoothly forward.

Leo: [Cooing]

Steve: Yeah.

Leo: Or you can do what I do and use nails; right? That's what Web3991 said.

Steve: Or get some glue. Oh, that screw is gone. Get some glue.

Leo: Nothing like Krazy Glue. You know, I actually had the worst - this is complete digression.

Steve: Hey, you know, we're done now. Although I did want to say I finished the third of The Rho Agenda books. Oh, my god. We talked about it last week. They're all three available on Audible.

Leo: I've got to read those, yeah.

Steve: And by the way, Honor Harrington books and something else are on sale right now for $4.95. So I wanted to bring that up, too. But The Rho Agenda books, if anyone is starting in on them, I would consider the first two books foundation for the third. The third one is very difficult to stop reading. GRC almost didn't get a new server last week. I'm not kidding. It is so good. And it finished with some surprises. So it ends up I didn't really endorse it strongly because I didn't know how it was going to turn out. I was only 75 percent of book three. I finished it. Wow. It's really fun. And remember you said you were going to jump on it, Leo, because it was an alien spaceship began to alter three teenagers. And we followed their antics. And it turns out that the spaceship had an agenda of its own, which is really interesting, too. So I do - R-H-O, Rho Agenda. It's just spectacular. And so you had a divergence. I'm sorry.

Leo: No, no, no. It was more about screwing than about...

Steve: Okay.

Leo: We're done screwing, I think. And we'll move on to the - I think it's the point well taken. Anything else you want to talk about?

Steve: I'm exhausted.

Leo: Where do you get your underwear?

Steve: What? Amazon.

[Laughter]

Leo: That is a leading question. I get mine from Manpacks. This is actually a new sponsor on TWiT, just kind of for fun. I actually found out about Manpacks from Jeff Jarvis. It is a place where you can order underwear by mail, and other manly goods, and you get a new ship- what you do is you create a Manpack...

Steve: Wait. These are - this is a new sponsor for TWiT?

Leo: Manpacks.com. Well, you know, it's a fun little sponsor.

Steve: Okay, good.

Leo: But I like it. And I've been using it...

Steve: Given our audience, I think, you know...

Leo: They're mostly men. And they're packing. So the idea is - let me show you. Actually let's see if I can log into my Manpack.

Steve: [Laughing] Hey, LastPass will do that for you.

Leo: It will. It just did. I love Manpack. I'll tell you why I like Manpacks. Because there's certain things you want, just like razor blades, you know you want on a regular basis. And so what you do is you set it up, and then you get it automatically every three months, or more often if you want. And it's just convenient. So I'm getting cushioned crew socks, boxers, shave oil, shaving cream...

Steve: You go through a lot of those, huh?

Leo: Yeah. You know, I get three new pairs of underpants every three months, and I throw out the oldest three.

Steve: Perfect. Just recycle it.

Leo: Yeah, recycle. I don't throw them out.

Steve: No, don't bother laundering them, just...

Leo: Well, you probably should since you're only getting three - one every new month. But they have all sorts of fun stuff. And you can change your pack. You can

get new stuff in your Manpack. You've got a dashboard. I should - let me see. Where can I find the other things in the Manpack? Well, they've got - here's something. They also sell vitamins. Because, you know, there are certain things that you need to take on a regular basis. I wonder if they've got Vitamin D. They are - we're talking to them. We're going to make sure that they have everything that Steve Gibson recommends.

Steve: Hey, cool.

Leo: So here's the deal. Manpacks.com/twit. You can get $10 off your first purchase of $30 or more. And I think you could also get a gift card, a $50 gift card for 40 bucks so you can see - I'm trying to find - you can see I've been a Manpacks member since August 2011. Started with underwear, but now it's everything. I'm getting...

Steve: You have been?

Leo: Oh, yeah. That's why we're doing this.

Steve: Oh, cool.

Leo: Because I'm a fan.

Steve: Apparently. And I guess your underwear has been working for you.

Leo: I - yes [laughing]. Where is my shopping list? I want to show you all the different things you can get. Socks - oh, here it is. Visit the shop. There was a big button, and I didn't even see it. So here's the Manpacks shop. I don't know. Are you a boxers or a briefs kind of guy?

Steve: You did ask me last week, and I wondered where that was coming from.

Leo: Yeah. I'm a boxer brief guy. It's like a mix of both. [Laughing] I love this. Anyway, I just thought I'd mention this. Manpacks, socks, grooming items. They even have Sir Richard's Extra Large, if you need them. Whatever you need.

Steve: Sir Richard's.

Leo: Yeah, I know. Isn't that a good name? Sir Richard, yes. I just think the service is great. It's like Zappos for underwear, somebody said on Twitter, and I agree. So use the offer code. We'll make a little money. You'll save a little money.

Steve: Hey, save some, yeah, save 10 bucks.

Leo: Manpacks.com/twit. I just wanted to mention that.

Steve: I'm so glad we didn't finish the podcast without that.

Leo: [Laughing] Steverino, that was fun. It was so nice to meet Brian. I've been a fan, and I told him before the show, I didn't say it on the show, but I told him before the show, since - I didn't realize he'd left the Washington Post three years ago. He was saying it's been a great thing for him.

Steve: Yeah, I noticed about a few weeks ago that he had an anniversary that he mentioned, and it was his three-year anniversary. And as he also said to us before we began recording, it's the best thing that ever happened. He was there, he'd been there for a long time, we used to watch him and follow him there.

Leo: Oh, yeah.

Steve: Then he set up his own deal with KrebsOnSecurity, and he said, wow, it's working. It's the best thing he ever did. So, you know, I'm really, really glad we had him. I think he really brought a different perspective and lots of really cool information to our listeners.

Leo: Yeah. I learned so much from him over the years. And what is sad is that he was one of the, I think the only guy in mainstream media who really gave serious security information, not, you know, update your antivirus kind of level.

Steve: Yeah. I'm glad I remembered that it was from him that I got that fantastic piece of wisdom, which is never install something that you didn't go looking for. That was Brian.

Leo: Right. That's one of his three rules, yeah.

Steve: Yeah.

Leo: All right. Let's see. You can watch this show, it's 11:00 a.m. Pacific, 2:00 p.m. Eastern. I'm sorry, 1:00, yeah, 2:00 p.m. Eastern on TWiT.tv every Wednesday. That would be 1900 UTC, if you're outside the U.S. It also is available on demand, after the fact, audio and video from TWiT.tv and wherever you get your Internet broadcasts. We're everywhere. We try to be, anyway. Oh, we're on Roku now. We've got a great iPad app, a number of great iPad apps, a number of great Android apps. It's really, it's easy to find TWiT, so just look around. And we'll be back next week to talk more about security. A Q&A episode. That means you need to go to

GRC.com/feedback, if you've got something for Steve. People always say, how do I ask Steve a question? That's how.

Steve: Yup.

Leo: GRC.com/feedback. While you're there, take a look, and you'll find SpinRite, the world's finest hard drive maintenance and recovery vessel, software that you must have. If you have a hard drive, you'd better have SpinRite. ShieldsUP! now updated for that UPnP exploit, so you can test your servers there, your router. Lots of free stuff, too. GRC.com. Steve also has 16Kb versions of the show there, and text transcriptions by a human being.

Steve: Yes, who is under snow at the moment. Elaine sent...

Leo: Where is Elaine? Is she in Northern California?

Steve: No, no, she's - I have no idea. Wherever it is, it's the extreme weather capital of the continent. It's some - like she's in the desert somewhere.

Leo: Oh, high desert probably, sure. Gets very hot and very cold, yeah.

Steve: Yeah. So she's got, like, swamps running through her house, or she's like buried under snow. She has a satellite Internet connection, which is always - that's why she wants the lower bandwidth audio from me is that she's got bandwidth caps on her satellite feed. I mean, and I think her husband is on, like, a bicycle with a generator.

Leo: We're getting it now, Elaine. It's coming down. Here it comes.

[Elaine collapses here in helpless laughter]

Leo: Pedal faster. Pedal faster. Here it comes. I can see it.

Steve: Yeah, so, I mean, and they've got a whole bunch - they've got dogs and horses and, like, bats and owls, and it sounds like a menagerie out there.

Leo: They don't keep bats. They just happen to have them, I'm sure.

Steve: Oh, no, I wouldn't be surprised if Elaine has...

Leo: You don't want to keep bats.

Steve: I don't know.

Leo: Seems like a bad idea. But I could be wrong. All right, Steve. Great fun. Thanks a lot.

Steve: Thanks so much. Talk to you next week, Leo.

Leo: See you next time.