Hello I'm Roger safe in today's Thursday, April 11 and you're listening to the information security news podcast brought to you by Northwestern University information technology. Don't forget it's coming up to tax deadline April 15. United States so adultery to do your taxes but also don't forget that it's a lot of bad guys out there trying to steal your personal information and they may be doing it by trying to send you a message and all that purports to be from the IRS so be careful about opening a messages about this time especially if that messages can ask for your personal information, start by having some tech tips you know I've got a couple different articles all kind of like the same but all with different things the first when here is 10 good tech habits everyone should have these of things we've talked about before backing up your machine and things of that nature always always a good idea and the augment this I've got to know the top 10 iPhone security tips also things that we've talked about before you know having the pass code for example on your iPhone and stuff like that and then I also found one more was a dozen tools for removing almost any malware and yet you know if you listen to this podcast for any length of time I really like it when they put these things together I don't know why but I do and I think the reason I like it is it's just very convenient to be able to grab a single article that sub deals with the problem that you might be experiencing an habit offering solutions because a lot of times it especially tech world in a sailor I have problem may is a missing all well you know I didn't be in that solved it and that may very well be true be work for them but be may not work for you so it's kind of nice to have an option CNN option DEM ill various other options that you can that you can do to us solve whatever problems that you got sorry likely together these of these things up and it's good would learn some information as well so have links to all of these in the show notes at the on the website be sure to go check that stuff out and I were to talk little bit about ran somewhere now we've talked about ran somewhere before and it's becoming more more popular and essentially what this rants warriors is bad guy gets you to put some malware on your machine however that happens right and there is a usually a yoke of an official looking page that pops up on your screen that says you know the FBI is investigating you we've determined that you've committed this crime and were in a combined arrest you you got 72 hours to pay us to honor dollar fine otherwise were to lock you in a lot of people when they see this it's like all my goodness you know I don't know what I was doing but it's certainly not worth getting locked up for so I'll pay the $200 and that's ran somewhere and the FBI clearly does not do this stuff but bad guys do an bad guys know that good people will fall for this kind of a scam and no bill pay up so ran somewhere has become really popular really start taking off last year and it's becoming more more popular this year so the couple different articles that all deal with ran somewhere here and the first one is look if this happens to you here's how to get rid of it without actually funeral pain the extortion money bet that bad guy wants so that's great and lots of different tips that you can use in order to insanity get your machine back after you got rats were on it and then the last thing is an article that double-click team comer he put out and it was it basically talks about ran somewhere and how works in so you've got you've got some screenshots of what it looks like you've got the you know he kind of talking with somebody that's very close to the topic you know and so was talk to the in of people on the other into her click in the money and things like that so it's it's it's very interesting to read the stuff and I think that this ran somewhere is going going to become the issue you know it's one thing to to infect the computer with malware of some
sort for a lot of you know the bad guys at the that's great it can use it is part of their bond that and they're quite happy with that but money makes a lot happier if they can get you know 5000 $200 on a somebody there to do that don't talk about an identity theft case at the University of Florida and University of Florida and identity theft situation and it turns out that it's actually one of their employees now this this causes all sorts of problems I may not only for the University and for the people that were involved in their written to moving traffic but it which causes problems outside no more more people want to try to figure out ways where they can stop this stuff and that's all fine and good amended this is good as some kind of strange coming from the offscreen podcast but you know it's very difficult to stop in insider from doing something that they're not supposed to do you know copying files to know writing down information ammunition when people are determined to be bad there's just not a lot that you can do about that that being said it does make sense when you've got information like this to audited on a regular basis if you can look at the log see who is accessing it when they were accessing them why were the axis sing it in old these types of things can all be done and in some cases can be done automatically so that when there's a problem security staff gets notified right away I think that's what we really need to get more of here in a limitless stop somebody from doing bad but you have to be aware of when somebody does something bad you have to be have an opportunity to see that they're doing bad that think that's where we're falling down on the job right now we don't see that they're doing bad until you know the Vardy done it and that's clearly not acceptable enough so that I mean a Nestlé pickle University of Florida here comes the same thing could happen anybody but you know since they happen to be the one story was about I guess I am picking on them little bit and then I read a story here about malware in us is 92% of attacks the zip files are used to deliver the malware and this is from a company called fire I and I do this tell you based on the malware that we see here most of it is 92% of it clearly not coming from zip files we get attacks that are based on zip files to about it but a lot of the malware that we see seems to still be drive-bys in oh where a person goes to a webpage perfectly legitimate webpage some to convert webpages infected things of that nature it's just that kind of thing and it did to me whenever I see a statistic that is so unit 92% of the love of this unlike really 92% is an awful lot in oh I mean even if the Trident gum company could only get 4/5 dentists to recommend their gun that's only 80% and even a think that's a lot that's a big number to get 80% of anybody to agree on anything and I got 92% that doesn't necessarily mean that this study is you know complete nonsense and it does point out of a really serious problem that is the zip files being used to deliver malware and it happens regularly in fact I saw some of it today so it's it's out there got be very careful with stuff like this here and then there's a store now and I never I never heard of the store before in that's what actually maybe caught their eye it's called Vishnu markets and probably misspelling that SCh and UC case of markets I guess it's a story you know kind of like a jeweler Dominic's or something overhears it is my understanding and it looks like they were hacked and it looks like they were hacked on their their credit card terminals to point-of-sale terminals and use another is also struggling all you not only to have the identity theft issues over here but she looks is a level I merchants in a PCI that means monster finds potentially and the gum I'm going to assume either I don't know for a fact that they if their level I merchant they've must've gone through an awful lot of food summit level I merchants you have to have scanning you have to have regular auditing
Donna means you have to have is a whole series of things and so what I you know I think is interesting about this is you could potentially be doing all of the things that aren't that are necessarily done following the standard and just because you're following a standard does not mean you're not going to have a problem standard help to minimize the problem the standard helps you address the problem when it occurs but following the standard does not necessarily prevent you from having the problem nine but I actually hope that if they were PCI compliant net worth on the standards that the there's no monster find here as it does seem like PCI that's the one thing that they really use is a big stick of you million-dollar fines and I think that it was time to find people this time not to and if there following the standard don't think there should be Brian Krebs is an interesting article to about the things that you read online and fake this kind of comes in the is important because some of the other things I said today in a likely mention the IRS scams are the the ran somewhere in things like this and this is just about things or to read online and you know the sort of relationships that you build with individuals that you've never actually met some kind of interesting it's it I won't give away the about as good Krebs always has good stuff I thought this article was particularly interesting so give it a whirl then there's a story here that what catches my eye by it's about banks and basically what it turns out is this a new set of of laws the consolidated and further continuing appropriations act of 2013 which basically funds the federal government and somebody slipped something into this here you know commerce minutes senators I believe while laws ring committee can anonymously slip in amendments and somebody I guess was concerned about Chinese hackers and so they anonymously slipped in an amendment to this law that basically is to make it very difficult for places like Department of Homeland Security to make purchases because they have to do these audits in order to make these purchases and unfortunately it seems like part of the requirement to do these audits requires you to make these purchases that you can't make now because you can't do the audit and so you know there's a part of me says you I appreciate that somebody is trying to do good but this idea that you can anonymously put something into a piece of legislation in the gets voted on that's crazy that needs to stop and you know I hope that there's enough blowback from something like this that that's what comes out there I guess is knowing our government nothing will change but it would be nice if something did this particular case also want to point out that there's problems with the Linksys home routers the busy and 600 is one of my bring this up because I just wanted than 600 not that long ago so I had one at home there's I believe there's an update for right now so I'll put a link to that of the show notes and then the somebody put together a story and a basically what they've found out is the average individual is more concerned over Facebook issues than credit card issues and vitamin A more concerned over the privacy of Facebook than they are concerned about the privacy of their credit card transactions for their credit card information and at least in my mind you know Facebook in a while Facebook CEO certainly got its issues out there credit card that's much more important to me the Facebook so kind of interesting and it's also kind of interesting to read the list of companies that are jockeying for position in the computer security field these days and amongst them is Google and a few years ago I don't think I would've seen Google as a computer security company but now Google's Peter security company interesting stuff here so go ahead and give this a whirl and you know I I I to stick is kind of interesting the way that the all the stuff is constantly evolving and I want to and with the kind of the
story basically this is a in interview online interview with the real bad guy guy who runs a bond and you know kind of talks about what he does he know goes to work holds down a regular job but then at night you know decides he wants to blow somebody off the Internet and doesn't he might be doing for money during the see it's it's interesting because he walks you through the kind of tools that he uses how he affects the machines when it's it's on really pretty fast any it's it's not furry often that you get chance to actually talk to somebody that's doing bad things in kind of a coherent reasonable fashion and this is certainly that kind of conversation I found it completely fascinating reading it anyway thanks for listing if you have any comments or suggestions please feel free to send in our deck safety in the northwestern.edu is always to find additional security information as well's notes to contain the links for today's podcast@herwebsiteWWW.IT.northwestern.edu/security