Hello I'm Roger safety in today's Friday, February 15 and you're listening to the information security news podcast brought to you by Northwestern University information technology starting with the updates there is a touch Tuesday just this past Tuesday for Microsoft and they had the baton of 57 vulnerabilities were patched on Tuesday so make sure you grab it looks like there's 12 different updates that fix a variety of holes in different system so looks like just about anything you have for Microsoft good chance there's an update for it so you want to make sure that you grabbed that stuff and that a lot of those things were pretty soon pretty serious vulnerabilities to so sick anything that you don't want to let the sit by two long-lived that's probably true for most is update site you probably say it again as I talk about some this other stuff via Adobe has got issues as well that we talked before about issues with the Adobe flash player and it looks like there's a new update out for flash that is going to take care of a couple of problems including widely we talked about last week so that's good as well there are some also subseries issues with reader an actual acrobat the these updates just came out recently I want to say today or maybe it was yesterday 'it's actually today that the updates just came out so make sure you grab the stuff especially for reader reader is something that is you know you're use it a lot and it's widely exploited on the net and speaking of Adobe and reader there's a real interesting story here on Ars Technica least I think it is about Adobe just spent time talking about them they made a big change to the way readers could do stuff and they were going to have something that will call protected view on their own reader and it was good to help prevent malware from spreading via reader which is great I mean that's really powerful right but it turns out that by default it's not turned on it something that you have to go and turn on yourself and you know most users to start to do that so we Adobe why right you have all of these problems it's not like this is news to you your products have penned being attacked constantly and then you put something in there to make things better and instead of turning it on and as the default you don't that's just that she's bad so fix that Adobe if you happen to be listening and if you're not Mr. Adobe and you can't fix is it Lisa can fix it for yourself actually go in and you turn the Renaissance of that you've got some protection again it's it's not enabled by default so you have to take care of it yourself how Microsoft cannot will report that I thought was sort of interesting as well this is about cyber security on a global landscape and sort of what they're trying to is what countries are have the most malware infection and how do they stack up when used with treaties and stuff and so it's it's interesting that places that are in a lot of treaties at least according to them have less malware now what I sort of took away from this report is a turns out that countries where lots of treaties lots of law you know stuff like this here less malware also less piracy of software in when I read this report essentially that's what I'm really reading is that Microsoft put this together initially because what they were trying to show us look countries you know in Western Europe for example have less piracy and they're trying to show one of the reasons they have less piracy while they have because they're in the street is I don't know if you can jump to that conclusion I don't even know if you can make the conclusion that less malware is make sense because during these first treaties it is just an interest report though but statistics being statistics you know you can get that whatever you want out of its supper link to the report the show notes you can take a look at it yourself wired to the map real interesting article from Ken VanWyk as you know I like Canon and he's got a story here about should you jailbreak your iPhone and you know Jill breaking that's where you set your
phone up so that it's no longer using all of the Apple provided software and falls in oh you can you can do things there that when a jail broken phone that you probably couldn't normally do a very common thing that you might want to do with Jill breaking his instead of downloading your apps from the iTunes Store you can download apps from you to Roger's house of apps you know that that's pretty common sort of thing that people want to do now that's really convenient and I like ping able to do that on the other hand there's a lot of risk there some jail breaking your phone is something that whether it's an iPhone and android whatever this is not something that for the weak of heart but A's got an interesting paper about it so you don't take a look at it and the I think you find an interesting article whether or not you want to jailbreak your iPhone that's up to you why were also talking about it the iPhone I paid by eyes swore that one looked at this article I thought this is God just be an old piece of news from a few years ago in a turns out no it's brand-new piece of news and it's the same sort of vulnerability on the iPhone that was there a few years ago it turns out that there is a vulnerability on the iPhone that can allow anybody to bypass your password stuff like this and access your phone and it's just a ridiculous sort of thing I'm trying to define the exact keystrokes here but something like you know making an emergency call hole holding down the power button twice canceling the emergency call in and just pops you in to the phone a minute of probably missing a step here but I'll post a link to a new check it out this very same thing happened just a couple years ago were there was some silly little way where you could bypass the via security password on the iPhone just ridiculous Apple what is wrong with you how can you even allow something like this take place and why don't you have a fix out for this like like yesterday this is just completely unacceptable behavior so Apple do something about this and the than I read a story that really caught maybe it's about hacking the line laptop docking station no real economy about this is I use a docking station at work story camping and I do have a laptop and take a back-and-forth between my home and my office and the you know it's nice that this plot the laptop and the docking station got a great big monitor keyboard or mouse everything is ready to go and there's an article by hacking that docking station no I'm not necessarily sure that hacking the docking station is really the right verbiage that I would be using here essentially what they're saying is look if you do something to that docking station in you know the put keystroke monitor you or something like that on the docking station you can't have access to the machine which is true enough yet if you have physical access to the docking station I think is one of the is important here maybe that's almost as good as having physical access to the machine so it really did get me thinking alone that you I never really gave any thought my docking station there it is sitting on my desk and the spry true for a lot of a lot of folks here answer think this is good be a presentation that blacktop black cat so very interesting output of blood and link to the show notes you can take a look at it might give us food for thought than other notes from the put in their those looking for something it works at the office for national counterintelligence executive which I didn't even know we had something like this in the government but it turns out that we do and they actually had a couple of documents that I thought were useful it's a lot of stuff that we've talked about but I'll I'll put links in the show notes again the first one is test practices for keeping your home network secure and against lots of things of Artie talked about but it's small document at that thing was 456 pages of the like that and then another document that I thought was really nice for traveling overseas with mobile
phones, laptops, PDAs, and again just couple page document about things that you can be
doing there and good good information note were often talking about you know I have a
real aversion to online banking and you know about all the fraud that goes on over there
in this story about $200 million in credit card fraud scheme just caught my eye and the
other again good information or thoughts that they could be arrested somebody with
25,000 credit cards 45,000 credit cards that I had all these different identities and people
working foreman innovates just it just crazy how this stuff works and sort of what got me
about the story is not that the numbers originally but just like all the details about how
this credit card fraud takes place and I really did you know it really annoys me that the
banks don't do more about this I don't know if you've ever had your credit card
fraudulently used but I have and the you know most of the time they just send you a new
car didn't be no don't worry about it and his near as I know they never even try to track
people down you know it's it's just ridiculous that the credit card companies either they're
making way too much money off of Esso they just don't care because the money they're
making certainly covers these losses or you know there's somebody who's totally
negligent or maybe both is true but it's really shocking the way the credit card companies
handle these kinds of things and I really wish they would crack down and that might
make credit cards little less secure by thickened and people would be more secure than
one talk about the present Obama speech the other night and he just before he gave the
speech he issued an executive order about cyber security and so was in the press a lot in
in a cesspool of time reading and reviewing it and here's my take on it look this doesn't
mean a whole lot right now it sat there talking about setting up a framework where
government agencies and the private sector can share information they've been working
on things like this for years with the various eye sacks you know I don't expect that any
real change to be happening here now you may in fact see things differently you know
take a look at the notes take a look at the bill and not heard that the Executive Order sutra
sex the out there I think partially that what the president was trying to do here was get
some of the information that was maybe less controversial in the cyber intelligence
sharing and protection act assist the bill is been hung up I think he's trying to get some of
the things that's less controversial about sharing information to just happen and and and
happening quickly and and what I say quickly I mean quickly in kind of the glacial term per -
itis don't think any of this is can happen right away but we'll see what happens and then
somebody hacked a emergency alert system this is the thing that you might have that the
puts a bullet weather alert tornadoes warning for me it happens at home all the time when
it snows and details about the parking restrictions somebody hacked some of these things
in Michigan and Montana to broadcast a message to everybody that said the bodies of the
dead are rising from their graves are attacking the living clearly that wasn't happening
you know these kind of emergency alert things you really do need to protect them
because when something like you know you could get people to do all sorts of crazy
things and because they trustees this is post you know you but at least when I grew up in
a we were told if you know you hear these air raid sirens or something like this here and
you not accept its it's the Russians are attacking us for any new duck and cover right and
now they use those air raid sirens for everything will these emergency alert systems are
the same thing and I were told stay tuned to those emergency broadcast and follow their
instructions and you know you got a make sure that those things is secure one and with
quick programming note here the podcasts can be taking some well-deserved vacation
time store next podcast B on March 14 stay secure until then thanks for listing if they have any comments or suggestions please feel free to send them to our – safe in a northwestern.edu and is always defined additional security information as well's notes to contain the links for today's podcast at our website Dubya Dubya Dubya.IT.northwestern.edu/security