Hello I'm Roger safety in today's Thursday, August 1 and you're listening to the information security news podcast brought to you by Northwestern University information technology our first story has to deal with the Lenovo PC and it turns out that are of security agencies are reporting that there's a backdoor probably installed by the Chinese government on Lenovo PCs and they are prohibited from using them in their work not only it is that apply to our governments security agencies but also to a group called the five eyes which is Australia Canada New Zealand the UK and the US and none of them can use these these PCs is of these backdoors I don't know anything about the back doors to be honest with you now know if it exists or doesn't want to take them at their word and assume that that does exist but it will save that seems like lately whenever you buy a piece of equipment you know whether it's Lenovo or HP or Dell are you know you name it they all calm with all sorts of software built into one that's phoning home you know to keep track of your printer reading Gore in oh of time to do your BB video backup using our service that that you could have to pay for meters is all this extra croft there and I really do wish that you could order a PC and just just get the PC right you now get the machine have you know you're operating or operating system installed upon it and the and none of this other stuff and our youth we really makes me crazy that that's it's different all the time it's different everywhere and don't necessarily think that that's what this is but who knows in other so much stuff going on there sometimes it's hard to figure out what's going on by Yap Baghdad deftly I would silence if you're concerned about security like the work that you're doing is really really important I would take is a pretty good sign if if government agencies have decided they can't use a brand of equipment because it's dangerous for them to use few doing work that's of a sensitive nature I don't think you should be using it either now backs sticking with the government for second here the Pentagon says that Asian spies were are are targeting the radiation hardened electronics and what it turns out it's is that they're looking for you know the plans and equipment stuff lithosphere that for these radiation hardened electronics and you know my guess is they're stealing all sorts of stuff right of me despise this is what spies do they state they steal stuff they give to the government hopefully the government gets a leg up on development without having to invest all the dollars into it that the funeral the organization that did the development did but what worries me about this particular store in the reason up put it in there is you know if you talk about radiation hardened electronics what I read that to be and what the article essentially says is that talking about electronics to Connect Can Stand an Attack Radio and a Nuclear Attack the Electromagnetic Pulse That Will Take Place after the Attack Which Is Expected to Fry A Lot of Equipment If Not All of It in the Indy Area for Miles around Where and When the When the Bomb Goes off You This Kind of Worries Me Because It's Sort of Suggests That You Know Maybe Somebody's Planning on Doing This You Know Setting off One of These Bombs Have in the CMP Wiping out All This Equipment but They Want to Have an Infrastructure That Can Survive and You Know This Was Meant to Rouse One I Really Don't like the Idea Being Nuked Number One and Number Two I Really Do Hope That We Are Doing the Same Thing You Know Our Infrastructure Needs to Be Strong Enough to Solve to Stand up to This Kind of Attack and Solve Problems That Come up from Just Natural Disasters of Me Whether the Hurricanes Volcano You Know You'd You Name It on the We We Have To Build an Infrastructure That's Very Robust and If We Don't You Know Worries Me That Something Is to Come along and Infrastructures
Gone in This Day and Age You Know It's Pretty Tough Not to Have Sale Electricity for A Few Days but Could You Picture If You Didn't Have You No Telephone Service and Phoned in the Four Months You Know That Would Be Pretty Pretty Tough At Least I Think so so I Hope That Our Structures Being Well-Designed and Well Protected the Other Was a Story That We Had A Few Weeks Ago about a Faculty Member in the UK Does Release a Paper about the Encryption Algorithm on Keys for Cars and Porsche Went to Court and Got an Injunction so He Cannot Releases Is Documents That Says How the Encryption Algorithm Works and It Turns out This This Algorithm Is Used in A Lot Of Different Cars and the in You Know Essentially What They’re Worried about Is Bad Guy Gets a Hold of This Bag Is Going to Be Able to Duplicate These High-End Keys at a Relatively Low Cost and Basically Steal Cars All over the Place You Know I Agree That's Us That's a Serious Issue and Hopefully You Know There's a Delay in the Paper Here What What I Didn't Hear in This End in the Seer Is Yeah That's a Serious Issue and We Need the Time in Order to Come up with a Solution to to Fix This Problem so We Can Get It out to These Vehicles before They Become Vulnerable All That I Hear Them Doing Is Saying We Want to Stop This Information from Getting out There and I Had a Type My Guess Is That This Information Is about There Are Ready There's Been A Lot Of Publicity about It It Will Be out There Soon Sire Really Do Hope These Auto Manufacturers Are Taking This Time to Look to See How They Can Protect the Cars That Are Already on the Road Not Just the Cars That That Talking about Building the Future but Protecting the Cars That Are Already on the Road You Guys Gave Us a Car Key and Its Post A Lot the Door If It Turns out and Hit Anybody, the Door at Surreal Problem and You Guys Need to Adjust Address It Now the Feds Identify Some Russians Were behind Some Cyber Thefts.Turns out the Guy Is Already Are Some of These Guys Are Already Imprisoned and but These Are Massive There That's That They Took Place in in One Case 160 Million Bank Card Numbers Now That's What I Mean 160 Million Think about It the Hook That's Big Numbers and I Don't Even Know Should Do with It Was When You've Got a Database of Stolen Credit Card Numbers Attached That Stitches Just Boggles the Mind That You Could Have That Many but They Did Hundred 60 Million of Them They Had the Broken into NASDAQ They Had All Sorts Stuff. It's Just Amazing the Amount of Damage That Can Be Done by These People and It's You Know What What Kind of Really Worries Me about This Here Is Some of the Organizations That They're Breaking into Have Invested Serious Dollars in Their Security and Their Security Still Gets Breached and You Not Looking Here at Northwestern in a We Invest a Reasonable Amount Money but We Don't Invest Nearly This Kind of Money If If It You Know and Am Wondering Even If We Did Invest That Kind of Money When It Would Help Us. Our Preachers I Don't Know I Am Glad to See That the Were Going after People and Where or Where Putting Them in Jail I'm Really Disappointed That He Takes Years Because in Unit You Not Look How Quickly Damage Can Take Place in Your Computer You Download a Virus to Your Computer Your Computer's in Trouble You Know If Not Instantly Pretty Close to Instantly and When It Takes Seven Years to Prosecute Somebody You Know by Then the Damages so Far Done Its It's Laughable Were Related to Be A Lot Quicker I'm Dealing with These Types of Things Found Really Interesting Story and the It It's Got to Deal with This We Know That This High-Stakes Poker Playing You Probably Seen This on Television Where They're Their Playing of Texas Hold 'em Poker for Big Stakes in It Turns out There's a Guy in Japan
Who won up about $105 million in these poker terms under $5 million to someone like me? That’s pretty good chunk of change they way this guy will win $105 million in a poker tournament in a turns out he gets arrested in Japan for trying to scam victims out of will is what’s being reported $4 million you know if you’re already got a pretty successful career playing poker were you looks like to make pretty good money why do you want to take the fee criminal career in order to try to make some more money or mean what was this person thinking you know he was also working with the android malware he had set up some bogus dating website seminaked this seems like a ill will have again what is the point here totally can’t understand it anyway I’m glad to hear that they arrested this guy and hope he gets woody’s got coming to a black cat and death, taking place right now and these are two conferences in Las Vegas they been going on for more than 20 years now there for a popular and devcon a black cat it’s you know specially black cat you know there’s all sorts of things how to spot the sad you know you know kind of packing on each other’s machines find insecure device and stuff and posting in a bulletin board those stuff of things while one guy was going to black cat put together you know kind of a checklist some best practice tips for how to make sure you don’t get hacked over there. Now my guess is most people list in this podcast are not going to black hacks but the tips are really useful anyway so putting them in my show notes and take a look at them this really good information I really think any time you’re traveling having these tips like this here is it’s a great idea so take a look at it you probably find it for useful there’s a nest came out with a documented NEW guide on how to prevent malware incident art malware does not handle when they happen it’s primarily directed towards organizations but like most of the this documents really well put together there’s a town of information may be the more information in the but it’s got a lot of good stuff there and it I encourage you to take a look at that as well that I want to close with a story about how to hack an IPhone 60 seconds is the title and this is something we also talked about a few weeks ago it’s something the side of the black and basically what it is by using a malicious phone charger these these researchers at Georgia Tech are able to hack an IPhone relatively quickly now this is in a lot of respects is somewhat scary mean it’s it’s it’s either resist a somewhat scary is obviously if you’re only using your own phone charger it’s you know your good be fine for this kind of attack but it does say to me that for relatively low-cost to think we spent hundred $50 and ordered put the parts together to make this phone charger of theirs for relatively low-cost summit can cause a lot of mischief $50 is not a lot of money and of what you can do is have somebody charge their phone of the new replace one other apps you know like chrome or Facebook whatever it is and once they use it powell thereof. The gap malware and you’ve got access to their device you know you can innovate use it for credit card purchasing. A go live banker subselect that you know all that that’s pretty scary so if you are using IPhone to my guess is it’s probably a poor ready applies to the PC and the android devices as well if you are then you know you probably want to be very careful use your own charger really only use chargers and places that you’re absolutely certain you know of your office for example stuff like that anyway thanks for listening if you have any comments or suggestions please feel free to send them to our – safe in a Northwestern.edu and as always you find...
Additional Security Information As Well so Notes to Contain the Links for Today's Podcast at Our Website Www.IT.Northwestern.edu/Security