SEI Cyber Talk (Episode 14)

What is Ransomware?
by Ritwik Gupta and Elli Kanal

Ritwik Gupta: Hey, everyone. Welcome to another SEI Cyber Talk. I'm your host Ritwik Gupta. I'm a machine learning research scientist here at the Software Engineering Institute. And with me today I have Elli Kanal. Elli, do you want to introduce yourself?

Elli Kanal: Hey I'm a manager of-- the technical manager in the CERT division. We do also data science and analytics here.

Ritwik Gupta: Yeah, and so, we're actually here to talk to you about today-- about ransomware. And I've heard a lot about ransomware. I wish I had something to hold ransom with, but I'm pretty poor as it is. But it's a scary thing. We've heard a lot of people complain about it, talk about it. There's been a lot of impact on various industries around the world, and since I know nothing about it, but Elli knows a lot about it, could you explain to me what this is?

Elli Kanal: Sure, sure and let's actually start by taking a step back a little bit. So, there's this thing called malware, and probably you're all familiar with this. There's a whole lot of different flavors of malware. What's malware? Well, exactly what it sounds like, mal-ware. It's stuff that's doing something malicious on your computer. And honestly, it can be even off your computer as we'll get to in a little bit. But broadly speaking, there's a whole lot of ways that stuff can get on to your computers. Sometimes, if you perform acts on your computer, you visit unsafe websites, you put things in your computer, USB sticks that shouldn't be there, someone sends you a file attachment that you open that you shouldn't have opened, you can get all sorts of software on your machine that you probably don't want on it, and it will do bad things.

So, when we're talking about ransomware, that's a specific class of malware.

Ritwik Gupta: Got you, okay.

Elli Kanal: Each type of malware can do different things. So, some malware can take all your personal files. Some malware can exfiltrate, which we mean take out of your computer and send somewhere else, but exfiltrate all sorts of information. Sometimes, it's more damaging, where it can actually-- there have been all sorts of instances of malware causing physical damage to systems. Maybe they were specifically intended to, maybe not. And other malware is just there to break things. And it can just-- maybe it's there for fun, or maybe it's there to actually get some sort of a benefit.

Ransomware-- the effect that ransomware has on your machine is it will take all the files on your computer, every single one of them, and encrypt it. What does encrypted mean? It means that without a specific key, you can't get access to any of that stuff. Now, where is that key stored? Well, the key is sort of locked on your computer along with the ransomware. So, what the person who made the ransomware has done is essentially take all your stuff, lock it behind a safe, so to speak, and you can't access it unless you work with them to pay the ransom.

Ritwik Gupta: So, let me get this straight. So, the idea is that it's a specific type of malware, which I could get by kind of browsing the web and having some malicious ad compromise my computer, or I plugged in a flash drive I really shouldn't have plugged in--

Elli Kanal: Yeah.

Ritwik Gupta: Or whatever. And the idea is it's going to take my files and then just I guess encrypt them, right? And so, basically, I can't access them. I couldn't decrypt it if I wanted to because I guess they're using industry standard encryption protocols.

Elli Kanal: Right, they're using really strong encryption that you couldn't just break by yourself.

Ritwik Gupta: Right, if I could, I'd be really rich. Also, I'd be wanted by the government.

Elli Kanal: And that.

Ritwik Gupta: And then the basic idea is that they are telling me that I should pay a ransom to them either-- what, give them a briefcase of cash or like-- and in return, they'll give my files back, hopefully, right?

Elli Kanal: That's the thought. That's the idea, and it's actually funny you say it that way. So, yeah-- so, to go through it one more time, it's simply something is on your computer. It's taken all the files you have, locked them up, and then you have to pay to get them back. There's been a couple interesting repercussions of this. First of all, the goal of ransomware for the people who send it out is to make money, obviously. Well, one thing which the early instantiations of malware-- of the ransomware realized is when you're trying to have people pay you money, it's kind of a pain. And if you have someone's grandparents, or if you have someone who never works with the computer, and all of a sudden, they can't access their pictures of their dog or their cat, they have no idea how to pay for ransomware. They know how to get access to their cat, their cat pictures. And that's what they want. So, when the people who made this ransomware created it, they were like, "Oh, people are for sure going to send us money." They didn't even occur to them people might not know how to. So, they actually had to set up tech support for people to pay their ransom. And it turned out to be much more complicated and expensive than the people who made the ransomware intended to. So, that was an interesting outcome that they probably didn't anticipate.

Ritwik Gupta: Right, and is there even any guarantee that they'll give me my files back? How do I know if-- let's say I was-- first of all, I know we're not supposed to pay the ransom. We don't negotiate with terrorists, whatever. But if I were to, what's the guarantee I get my files back?

Elli Kanal: So, there is no guarantee, obviously.

Ritwik Gupta: Okay.

Elli Kanal: Except the point of ransomware as a class of bad things criminals do is to make criminals money. If the criminals themselves don't actually give you your files back when you pay the ransom, word of that will get out, and then the criminals will have less success the next time they make a ransomware attack. So, there's interesting economic arguments why the criminals will ensure that, if you pay, you're going to get your files back because they want you to pay next time. They're going to probably try and infect you again in a different computer, and they want to make sure that you're incented to actually do that.

Ritwik Gupta: Got you. So, if anyone's out there trying to get my thirty-five thousand Corgi pictures, I will probably not pay, just saying. I could probably find thirty-five thousand more pictures. But basically the idea is that there's like this honor amongst thieves. If they weren't going to pay, then there's no reason for some grandma who's heard about these thieves who have no honor to pay the money.

Elli Kanal: Right, and one interesting thing which has also come out, as people have been storing more and more of their files in the cloud, storing of their content, Google servers, or on Snapfish, or choose your favorite server, right--

Ritwik Gupta: Yeah.

Elli Kanal: The computer is really worth what it costs to buy. So, if you can buy a machine for three hundred bucks, which you can easily do on any sale, and the person who is doing the ransomware is charging you two grand, in many cases, it's simpler just to toss the machine out and get a new machine and view this as the cost of doing business in the modern era if you're not being careful about how to do that.

Ritwik Gupta: Got you. So, the idea is that if my files are on the cloud, maybe they can't be-- maybe the ransomware can't hijack them because they're somewhere secure hopefully, and so-- but I can use my new hardware, and my data would still be safe is the premise, right? Hopefully.

Elli Kanal: That is the premise that hopefully by putting your stuff elsewhere, the place where you put it, they won't get attacked by ransomware. Now, it's interesting because as this has become more prevalent and more of a problem, we're seeing an awful lot of places that you wouldn't necessarily expect to get attacked by ransomware to be hit. So, one of the examples that came out recently was-- I believe it was the entire city of Baltimore was knocked offline as a whole bunch of these machines that were-- that run the government there got infected by

ransomware. People came into work to do whatever government business they had and to run the services that the city runs, and they couldn't actually access the machines. That-- you might say, "Hey, well I can't a whole city?" Well, it turns out the city is run by people, and people can make mistakes everywhere.

Elli Kanal: Right and their computers actually run critical infrastructure.

Ritwik Gupta: Exactly, and the more critical the infrastructure and the less access you have to it, you get some real problems. There was another interesting thing. I believe the name of the malware was called NotPetya. That is one word N-O-T-P-E-T-Y-A. That actually took out an enormous amount of ships. So, these ships are going back and forth across the ocean. They have enormous amounts of software on them. I think I remember seeing recently the standard car nowadays has around ten million, if not many more, lines of code in it.

Ritwik Gupta: Wow.

Elli Kanal: So, these ships are enormous with navigational software, and automatic motor control, and all sorts of other systems. And these things were attacked by-- or somehow the malware got on there, and, again, all these computers on these ships were locked up. And rather than being Corgi pictures as you mentioned, this is maps, and content of the ship, and possibly access to the engine, all sorts of important things.

Ritwik Gupta: I think Corgi pictures are right up there in terms of importance to me at least.

Elli Kanal: I'm just saying. Different people have different values.

Ritwik Gupta: So, what you're telling me is that basically the past few years the Baltimore Ravens, the reason they're doing so poorly is their computer just locked up. They can't do much.

Elli Kanal: I'm not going to say for sure, but I mean there's definitely correlations going on.

Ritwik Gupta: Yeah, okay. So, this sounds crazy. We talked about stuff, practical stuff, we could do like don't pay the ransom or get new hardware. But how do I just prevent this from happening in the first place? I don't want ransomware.

Elli Kanal: Right.

Ritwik Gupta: I don't want my grandma to get ransomware. She certainly doesn't know what to do with it. How do I prevent any of this from happening in the first place?

Elli Kanal: Sure, and it's actually worth mentioning, when you're talking about don't negotiate with terrorists, in many, many cases, the way people are removing the ransomware is simply by paying the terrorists in this case because the ransomware does such an effective job of what it does, of locking up these machines, if there's critical stuff on these machines, there usually is no recovery method that doesn't involve decrypting the stuff that was encrypted, kind of unlocking it so to speak. And that's almost always something you just accomplish by paying for it.

Ritwik Gupta: Or some sort of mistake on the ransomware's part, right?

Elli Kanal: Or some mistake on the ransomware's part, which usually results in an unrecoverable file.

Ritwik Gupta: Sure.

Elli Kanal: Rather than we can now decrypt the whole thing.

Ritwik Gupta: Sure.

Elli Kanal: So, there's an issue there. But to your point I don't want this stuff in the first place, how do I avoid it, so there's an issue which we've been kind of talking about a lot here at SEI, something called cyber hygiene. It's essentially if someone has a cold, so all the standard things, you wash your hands, cough into your thing, don't cough into your hand. Make sure you behave appropriately and don't get other people sick. Cyber hygiene is how do you use a computer without getting your computer sick.

Ritwik Gupta: Sure.

Elli Kanal: Or without leaking your own personal information, or without putting yourself or others at risk because of data loss. So, malware and preventing any kind of malware and ransomware is no exception, is very much in that line. You want to follow best practices. If someone gives you a USB disk-- USB fob that you don't recognize, it should not go in your machine. When someone sends you an email that you don't recognize, don't open the attachments. Don't go to websites that your browser says, "This website probably has malware." Even if you think that looks like a great link or something's really funny or you want to play that game, it's probably a bad idea. And these are basic fundamental techniques that we have for avoiding getting these sorts of problems on your machine.

Ritwik Gupta: Cyber hygiene is cool and everything, but when people just don't know what there is that you can use to be hygienic, how do you get them to still be-- how to do proper cyber hygiene? Like my grandma, we told her if someone gets you a weird email, just don't open it or just ask me before you do that. Then that's the way she does it. But as we go more and more in

terms of tech proliferation, and as tech devices go everywhere, there's some embedded devices like diabetes monitors and everything that are running embedded Windows, or other things. How do we get people to be cyber hygienic as a default rather than as something they need to be proactive about?

Elli Kanal: Sure, let's talk about that in two ways. So, for the personal user, if I have someone who is just using a computer for their own use at home for example. The tools that are available for the personal user are getting more and more sophisticated. So, Gmail is free. Everyone has Gmail. What people don't realize is the level of sophistication within Gmail-- I shouldn't say Gmail specifically because, honestly, many of the large providers--

Ritwik Gupta: Sure, yeah, yeah.

Elli Kanal: Have the same service. But the level of sophistication within the services offered by these large providers is incredibly high. And to that extent, it's usually worth taking full advantage of that. So, there's a whole bunch of browsers you can download for free nowadays. Those browsers will give you warnings if you're doing something the browser thinks is bad. Listen to those warnings. Those warnings are backed by an enormous amount of effort to protect you and to protect the stuff you have. When you're using an online mail service, when you're browsing the different websites, or when you're uploading things to different services, there's a lot of warnings they'll give you. You know, this is a spam email. You probably shouldn't click it. Be careful of this attachment. Hey, do you know where this attachment came from? If not, don't enable all features, for example. And maybe you shouldn't allow your computer-- there are things which the average user wouldn't appreciate is risky that actually is.

Ritwik Gupta: Right.

Elli Kanal: So, one example of that Adobe PDFs, PDF files, which is now a general standard. Those files are not simply a digital version of a print document.

Ritwik Gupta: Sure, yeah

Elli Kanal: Those files can contain all sorts of code that can do really almost anything to your computer. And when the programs that you run say, "This file came from an unsafe environment. Are you sure you want to enable all features," there's all sorts of potentially nasty stuff that's trying to protect you from. The same thing with Word documents or other sorts of standard business software. These are much more powerful than the average user appreciates and can therefore wreak that much more havoc than you would expect.

Ritwik Gupta: Sure.

Elli Kanal: And the message to users is be careful of that. I started talking about personal, and I kind of swam a little bit into the enterprise.

Ritwik Gupta: That's fine, yeah.

Elli Kanal: For enterprise users, take advantage of all these warnings that you have. Definitely listen to your IT people. They're not just there to annoy you even though it seems like they might be. You want to be careful to listen to the advice that they are giving you regarding protecting yourself from threats you might get, what is a suspicious or malicious email. And take this stuff to heart because, at the end of the day, even though it's inconvenient, that is the price of the security they're trying to give you.

Ritwik Gupta: So, somewhat on a tangent but related is-- so, a lot of the stuff that I use my computer for, a lot of things are just based on cloud services. So, I at least know that if my computer today were to get ransomware for some reason, I'm not losing a lot. I can just wipe my hard drive and reinstall my OS and just be on my way. I can just-- I can hit up Atlassian again. I hit up Slack again, get my files, whatever. I have everything I need.

Elli Kanal: Right.

Ritwik Gupta: What I can't wipe though is my phone, right? My phone has my pictures. It has my texts and everything. Can my phone get ransomware?

Elli Kanal: So, the answer is it really depends on how you take care of it, but I would say assume yes.

Ritwik Gupta: Okay.

Elli Kanal: Right and then let me actually extend that one more. My family went on a vacation a little while ago. When we got to the place which we were renting in, the refrigerator was Twitter enabled, which we found so bizarre why that would be. But it was. Why would I mention that? Because that means that refrigerator had an entire operating system that allowed it to do all the things a computer can do and then run Twitter as well. So, not just your phone, your car, your lightbulb potentially, your-- the electrical devices in your house of all sorts, and you're mentioning your phone, these are all things that are becoming now computers that are also doing other things. Someone made a great comment I saw online. We used to think of a car as a device to get you from point A to point B. Nowadays, it's just a portable-- it's a computer that-- computer with wheels.

Ritwik Gupta: Yeah.

Elli Kanal: Right? Your refrigerator is no longer a device that cools things. it's a computer that has refrigeration in it. So, as more and more of this gets on there, and as more and more of them get attached to the Internet, yeah, these things can become infected also. The same exact advice applies. When you're using your phone, if someone sends you an attachment that you don't recognize, don't open it. That may be able to run some software that can infect your phone. When you're browsing the Internet on your phone, be careful what websites you go to and pay close attention to the warnings that your browser gives you. More often than not, people are using their phone personally, but corporate phones are widespread everywhere. So, take advantage of all these warnings.

Ritwik Gupta: I know a lot of people probably think this cyber hygiene stuff is very reactive. There's bad people out there, and they want to do things to me. And when it happens, I was the target, and I can't do much. So, I think the idea that you're trying to push is it's not good enough to be reactive. You have to be proactive and actually be aware of the warnings that are in the environment that we are in, which is the Internet or the computing environment in general, and to actually just-- I don't want to say use common sense because a lot of it sometimes can be not common sense. Computers are just not fundamentally intuitive to use all the time. But just kind of if there's that sixth sense thing like oh, this is shady, probably check it out first before clicking on it or running it or plugging it into your work computer or whatever.

Elli Kanal: And many people might not have that intuition as to what is that making it shady.

Ritwik Gupta: Yeah.

Elli Kanal: If you come across a friend of yours, and as soon as you see that guy you see his eyes are all red, and his voice is real scratchy, and his nose is running, you might intuit, "Hey. that guy has got a cold." And you wouldn't-- it doesn't take such a huge leap to get there. The problem is when people are interacting with their machines, there may be something that is screaming out very apparently to anyone who knows the software, "Hey, this is really suspicious." But if you don't have that intuition, you might not know. And the same way that if you don't recognize the symptoms of this guy has a cold, you might get a cold yourself. If you don't recognize the symptoms of malware, or the symptoms of suspicious files, you might get sick yourself.

Ritwik Gupta: Got you.

Elli Kanal: As the people are getting more and more tech savvy, as computers are becoming more and more pervasive parts of-- new parts of the lifestyles, people are picking up on this more and more and especially in this context as the manufacturers are trying to build in more protection.

Ritwik Gupta: Sure.

Elli Kanal: You know, sneeze shields over a bar weren't always a-- over a salad bar, wasn't always a thing. We've now created that, and people are safer for it. These things that we build into our browsers or build into our email, very similar to a sneeze shield. Pay attention to it. Take advantage of it. The same way it would be really nasty for you to stick your head under a sneeze shield, don't do that in the context of your browser either.

Ritwik Gupta: So, basically, I should be-- I shouldn't disable my firewall. I should probably use an ad blocker when I'm browsing the Internet. And I should probably follow the advice of the browser when it tells me, "This site is unsafe. Do you want to proceed?" Probably say no, right?

Elli Kanal: SEI actually has a whole list of recommendations about how to be hygienic, what are cyber hygiene guidelines. We'll put links to that below-- beneath the video. You can definitely check those out. In addition, we've also had some other conversations on this topic. And we can share that below as well. So, you guys can try to get more familiar what are these sorts of warning signs that you get all the time.

Ritwik Gupta: Absolutely. Are there any other resources that you'd recommend the audience to go out and browse or something quick that that can pick up about ransomware or malware?

Elli Kanal: Sure, the one that I would recommend, we can, again, put a link to this below as well, so the United States government actually has an awful lot of interest in keeping its citizens safe. And there is some interesting resources available that the government has put out just to make people more aware how you protect yourself online. And we can add some links to that below.

Ritwik Gupta: Awesome. Well, hey, guys, thanks for joining us today. If you want more information on the stuff that we do, check out the links in the description. There's probably going to be an email that comes up that says info@sei.cmu.edu. If there's any questions, just email us. You can email us personally at rgupta@sei.cmu.edu or ekanal@sei.cmu.edu. But again, remember it's a dangerous world out there, and the best you can do is be proactive. Look out for these warning signs. And if anyone tells you to plug in a random flash drive--

Elli Kanal: Don't do it.

Ritwik Gupta: Probably don't do that, yeah.

Elli Kanal: Cool.

Ritwik Gupta: Anyways, thank you guys, and we hope you guys continue watching. If you guys enjoy what we're talking about, and want to hear more, get notified of each SEI Cyber Talk episode by clicking the subscribe button below. Also, if YouTube is not your thing, each episode is also available on the Cyber Talks pages on Apple Podcasts, Spotify, and I never get to do this, but you can also check us out on SoundCloud. So, thank you guys, and, again, hit the subscribe button below and get notified of every knew Cyber Talk.

Related Resources

The Untold Story of NotPetya, the Most Devastating Cyberattack in History (Wired)

What is Cyber Hygiene? (SEI Cyber Talk)

Cyber Hygiene: 11 Essential Practices (SEI Blog Post)

Ransomware Cyberattacks Knock Baltimore's City Services Offline (NPR)