Ransomware

Podcasting monthly from the shores of the Delaware River in Trenton, New Jersey, TechNJ brings you discussions and interviews on a variety of current technology issues, trends & topics with industry leaders and up-and-coming influencers. We will find where "Technology Meets Public Service in New Jersey".

JS: Hello, and welcome to TechNJ. I'm your host, John Silvestri. Computer viruses have been around almost as long as computers have, threatening everything from decreased performance to widespread theft of personal data. Worms, Trojans, boot sector viruses, viruses in documents, viruses in image files, viruses on websites – typically, when we hear about a virus or malware it usually involves the security breach where data gets leaked out to some nefarious party. That party could then sell it or use it and whatever way they see fit. Recently, a new method of attack has been making the headlines. Instead of stealing data, this new form of attack threatens to destroy data unless the hackers demands are met. This new method of attack has been dubbed ransomware and has affected home computers and large organizations alike. I have Krista Mazzeo, cyber threat intelligent analyst for the NJ Cybersecurity Communications Integration Cell under the NJ Office of Homeland Security and Preparedness. She is a certified ethical hacker, and has a Masters of Science in Cybersecurity. Krista, thank you for joining us here today!
KM: Thank you for having me!

KM: Thank you very much.

JS: So, what is ransomware? How does ransomware differ from all the other viruses that have plagued computer systems?

KM: Well, everyone's talking about ransomware now, but the down and dirty of it is that ransomware is a type of malicious software, or malware, that attempts to extort victims by restricting access to devices, computers, and files.

JS: So, how does ransomware get in? Does ransomware act like a normal virus to get in or does it have a special avenue…

KM: Well, I started looking into ransomware about a year-and-a-half to two years ago. I had heard the term and I found it kind of interesting and cleverly evil, so it fascinated me. So I started looking into the different types of variants, and they all act and perform a little differently. A common attack vector is through malicious emails, or emails that contain malicious attachments, or links that lead to malicious or compromised websites. That's a primary attack vector that we've seen, you know, the start of last year... the past year, year-and-a-half. Another attack vector is through malvertising. Now, malvertising is kind of a shortened form of malicious advertising.

JS: So if I don't like advertising already this is even worse.

KM: Exactly, exactly! This is actually that that added, you know, encouragement you need to run an ad blocker on your browser. What malicious advertising is, is when you visit a website, a lot of news websites will have ads… the problem is they're not hosting the advertisements. They're actually going through third-party advertising networks, so they do not have control over the ads that get placed on their website - they just kind of cycle through. So, hackers have actually attacked these advertising networks and have replaced some of the ads with ads that host malicious code inside them. So when you go to visit a website that you might go to all the time, and you've never had a problem with before, one day you'll visit it and all the sudden you're infected - not just with ransomware, it could be with other forms of malware too. You know, but then there's nothing that you've done wrong essentially.

JS: I've seen some of these. They appear very intrusive, and they also appear very alarming. You know, they'll pop up and say your computer is infected with 10000 viruses! Download our software immediately. Click “OK” right now or else everything's ruined. Like…

KM: That's a little different, that's called scareware…

JS: Aaaah…

KM: …And a lot of times if… if you've heard of ad ware that gets on your system, or spyware, adware will pop up advertisements on your actual system, and part of that they'll try and get you to act, and they do that through social engineering, psychological manipulation, to try and scare you into thinking you have a big virus on your computer. They’ll scare you into thinking that law enforcement has detected some type of illicit files on your machine, and you need to pay in order to restore access and clean your system. If it's not associated with the antivirus software you're already running, then it's obviously scareware and you need to run a scan.

JS: Back to ransomware though… So, you know, no fault of my own, I get to wear on my system somehow. How does it go about getting me and my files?

KM: That's an interesting process. Typically, once you get infected, the executable, the ransomware will run silently in the background. You probably won't pick up on anything if you're not looking for it, although there are cases where it will degrade system performance depending on the system you have and the number of files. But it gets on your system in a number of ways, it could be through a Trojan, a back door. It could be deployed manually through remote desktop protocol compromise. Once it starts, it performs a number of functions. It'll try and do what’s called maintaining persistence, which means it’ll inject processes in to, say, the registry in the startup, so even if you reboot your system, it’s still running. Then, it will search around for a bunch of different files that it wants to encrypt. Now, the developer of the ransomware kind of has control of that. So, let's say we know a photography company that'll have a lot of jpegs. Well, if we target them we're going to want to encrypt all their jpegs because that's their bread and butter right there. But, they typically go after document files, Excel spreadsheets, PDFs… anything that the variant or the developer of the variant determines to be important, that you pay to get back. After it does that, it will either propagate, it might look for other drives connected to your system or the network. it'll look for thumb drives, external hard drives, a network attached storage, mapped and unmapped network shares. It will encrypt everything it finds there. When it's done, it alerts you. It's kind of unusual in that respect because other viruses, they might not alert you right away, especially if there's malware that's trying to steal your data. It's not going to let you know that it's stealing your data. Ransomware goes, “Hey!”… we’re going to pop up a note.. “Guess what? Your files are locked! If you want them back, you’re gonna pay us x amount of Bitcoin in order to restore access. If you pay us, usually within a time frame, we will send you a decryption key”. Other ransomware variants have other, more nefarious functions where it will have a countdown timer on the ransom note. if you don't pay within a certain amount of time, it threatens to delete your files or exfiltrate your data, so those are other considerations too.

JS: So you get a message on the screen that says, “I want 10 Bitcoin and you get all your files back. I'll send you a decryption key”. What if, you know, I operate my photographer shop and I don't know anything about Bitcoin?

KM: You wouldn't be alone if that was the case, because there a lot of people that have never heard of Bitcoin that suddenly know about Bitcoin. And they suddenly know how to buy it because they had to figure it out. A lot of individuals, they'll call in Tech professionals, and at this point, you know, your IT service guy is going to at least have heard about Bitcoin, if not conducted a transaction with it. They'll know about it. But typically, the ransom note will give you instructions on what to do, and some ransomware variants actually have a customer service component. These organized criminal groups that are behind some of these Ransomware campaigns really want the victim to feel cared for, and they want to make sure they get their money, so the offer light a chat feature if you have any questions. They'll provide an email address to contact them if there's any kind of question. It’s kind of fascinating to see, but there's a whole economy that's built up underneath this type of malware.

JS: That's impressive, “Press 1 for customer service, press 2 to talk to a representative”?

KM: Pretty much, yeah. Hackers don't like using the phone so it's typically online, but yeah they'll be instructions on how to purchase the Bitcoin, which is the relatively anonymous cryptocurrency that hackers use to conduct transactions.

JS: Right, and I’m assuming Bitcoin is harder to trace then say non-executive $20 bills or something along those lines.

KM: Well, if you're going to send money you need someplace to mail it to, you need to transfer to a bank account and that is easily traceable. Now, I'm not going to say Bitcoin is completely untraceable, that is not true, but it is a lot more difficult to trace Bitcoin that it is any other form of currency.

JS: So you conduct the transaction with the gentleman hackers here who have so graciously told you how to give them the money, they just give you the decryption keys and they go on their merry way? That this just a guaranteed it's not going to be…

KM: You hope they do, that's not always the case. Criminal organizations that really have made a business out of it, I'd say 9 times out of 10 they will send the decryption keys or at least they intend to send them. In other fly-by-night operations or script kiddies that get ahold of some ransomware code and deploy it, cause once they have the money they don't care. You know, they're gone. They'll infect the next person. So, it's kind of a 50-50 chance you're taking after you pay, and the reason why I say that, not only does the hacker have the choice of sending you the decryption key or not, they're also a number of other things that can take place between the time that you submit payment in the time you get your key. Ransomware and the hackers behind it use what's known as a C2 server, command-and-control server. That's pretty much where they deploy all their operations and they can, you know, conduct their business and it's typically not a server they own. It's either going to be hosted on the dark web somewhere that can't be found. They might have hacked into somebody else's server or company server and stealing their resources to host their server to conduct these transactions. Well, the problem is once, you know, if there's an IP address is detected or a compromise server that's found and if it's cleaned and wiped or law enforcement takes a C2 server offline, that communication channel is gone. So you can no longer get that key with the way some variants work. I've talked to a number of people who have paid and they've waited patiently for a key that never came, so then you still have your… your files are encrypted and you're sitting there waiting for a key and you're out the money that you paid and the hackers long gone.

JS: And it's safe to say that once a file's encrypted you don't have that decryption key, like you can't put cycles you know toward decrypting a file just through brute force?

KM: There are a team of security researchers that I follow on Twitter that are at the top of their game in ransomware, and they actually take upon themselves and in spend a lot of their free time creating free publicly-available decryption tools for some variants. What they'll do is they'll try and obtain a sample of the ransomware's executable. Once they have that, they'll reverse engineer it and they'll try and figure out if maybe the decryption key is hidden somewhere in the code, or if they can crack it. If the encryption on that key is not that great, sometimes they are able to crack it and they will actually host a link to software you can use to decrypt your files. That is not guaranteed in every case, and a lot of times it might take months between the time a ransomware variant is discovered and a decryption tool is released. Now I've kind of made it my mission with the NJCCIC, we have an extensive ransomware threat profile up on our website at www.cyber.nj.gov. Currently, we're at 170 variants we have done research on. I list how each of them works, what to look for, how you know if your infected by that particular variant, as well as any free publicly-available decryption tools that are available.

JS: Is this limited to computers? Is this just strictly servers, laptops, desktops?

KS: Nope

JS: No?

KS: Nope!

JS: Is anything safe anymore?

KM: No, throw out all your technology…No, primarily it’s computers. Primarily Windows operating system is targeted. It's the most widely-used operating system and that's why, you know, the hackers are casting a wide net and trying to catch as many victims as possible.

JS: Right, the widest net with the least effort.

KM: Yeah, exactly. However, we have seen a growth in the Android operating system ransomware department. Android has been targeted. Some of their ransomware variants, they don't encrypt the files it's more of a screen locker. You just can't use any function on your phone until you flash the ROM or something like that. Android seems to be easier to overcome Android ransomware infections. A lot of times you just have to restore to factory settings, or something along those lines. Well, there's a story just this past December, where guy had gotten a brand new smart TV for Christmas and he set it up, and he installed an application on it to stream some sort of movies or TV shows. That application was malicious, he did not know that, and when it was done installing it popped up for ransom note on his TV screen

JS: (Jokingly) Usually goes come from the cable provider…

KM: Exactly! Popped it up and, you know, Merry Christmas to him. He couldn't use it, and he ended up… I think he returned it back at the store.

JS: That’s… wow.

KM: But, just think about all of the different devices that we now have connected to the internet. And in fact, The ransomware event that happened last weekend with a variant called Wanna Cry, there was a report that just came out today saying that they were medical devices that were impacted. Files on actual medical devices, something connected to MRI scanning or MRI injection, I'm not even I'm not a doctor I'm not sure… but those actual devices were encrypted impacted by ransomware. You know, people have wirelessly-connected pacemakers which, why would you do that, but I understand in order to manage those devices it might make it easier for the management team, but imagine if somebody, you know, encrypts somebody's pacemaker or threatens to. That's definitely a serious concern moving forward.

JS: Let's talk more about the Wanna Cry. This is something that hit the news, basically everybody went home Friday you know… went to enjoy the weekend, and over the weekend this thing stormed through what seemed to be everywhere, and everybody on Monday, you know, all systems alert, run Windows update, run all the update files you can.

KM: Right, batten down the hatches.

JS: So how did this all start?

KM: We started seeing reports coming in late Friday morning last week. You know, it was just a couple of tweets on Twitter talking about it and then, I'm like, "Alright, what's going on?". There's something, because more and more people are talking about it. Before we knew anything, we're hearing reports that 16 hospitals in the in the UK had been hit with this ransomware variant. A telecommunications company out of Spain was hit, and we're hearing all these reports coming in from other countries about this ransomware, and then as soon as some of the researchers started weighing in on it, they realize that this was spreading so quickly. Actually, this was most quickly spreading ransomware variant than anyone seen so far because whoever had coded it had done so to exploit the SMB1 vulnerability, which is a vulnerability within Microsoft that was announced, I believe in March, and patched in March. Microsoft rolled out a patch for that, and apparently a lot of people did not apply that patch or update. This was linked to an exploit the NSA reportedly used called Eternal Blue, and they supposedly use that to you know Target enemies of the country and try and see what they're talking about. Eventually, Microsoft discovered this vulnerability, or found out about it, did what they could patch it but a lot of people just were behind in their patching. We haven't heard that many reports of victims impacted in the United States. People are still trying to figure out why that is. But there were reports of 150 countries got impacted. Some of the numbers were, I believe, wildly inflated coming out initially because people just were trying to gather as much information as it came in and in some people got it wrong. But that was a very busy weekend. I was monitoring that all through Friday night till 2 in the morning, I'm sending alert emails out to my team my boss, and conference calls first thing Saturday morning to discuss it and everything like that so yeah, it was a hair-raising to say the least.

JS: So your team was on top of it the second the reports started coming out Friday morning, started monitoring, saw it build up and you just followed through…

KM: Yeah, we issued an alert to our membership right away on Friday. We knew that this was going to be big, so as soon as we gathered enough information that we felt confident about, we sent out an email to all of the NJCCIC membership to make them aware of it. We've gotten reports back that because we did send out that alert, it prompted people to take action right away and they were not impacted so.

JS: So, most people nowadays are running antivirus, their Windows update is set up automatic… This sounds very sensational, going through and infecting computers and pacemakers and everything. Is it really as bad as it sounds, or can I rely on my antivirus? Can I just fall back on, you know, my organization?

KM: No, not really. I mean, as a member of an organization, if you don't have any kind of control over IT Adminsitration, there’s very little that you can do with the exception of making sure the user account that you use to log on your system has restricted privileges. One of the things that ransomware variants often take advantage of are elevated privileges, or administrator access on user accounts. And unfortunately, this is a big problem and I think a lot of IT teams really need to sit down and seriously audit all of their users and see who's allowed access to what. If you have restricted access, that might stop some infections in their tracks. Antivirus, of course, I encourage everyone to run, you know, fully updated, a good reputable antivirus software. That won't catch all of them, because they're signature-based, and if there's a new variant out that nobody has any kind of signature to, it's not going to show up in any database. There's nothing to compare it to. It’s not going to be detected until it's too late. Other considerations include making sure that ports on your network and system that are not necessary are closed and disabled, and the reason why I say that is that over the past year we've seen an increasing number of New Jersey-based victims that got hit with ransomware through remote desktop protocol compromise. Remote desktop is a Microsoft-specific application that allows one user to connect to another computer remotely, and a lot of times these hackers will scan for open ports that are associated with common remote desktop software, and they will brute force it and get their way in. And what I mean by brute force is they'll compare password lists that they have against what's being used on the on the server, and see if there's, you know, weak or default credentials being used. And they’ll be able to get in that way, and it's super simple and super quick to crack passwords. I don't think people understand how easy it is to crack passwords, especially now the computer systems have so much processing power than they did previously. So it it takes a matter of seconds, what used to take days takes, you know, seconds or minutes to do. And they'll get in on server and deploy ransomware manually through the network. They’ll kind of map the network out, figure out where the most important files are, and they'll deploy the ransomware manually.

JS: So, for system administrators, lock down your system. Close off ports you’re not using. Shutdown services you’re not using…

KM: Absolutely.

JS: For end users, have robust strong passwords.

KM: Yes.

JS: Have a good password policy in place. Is there any other good information we can give out to people?

KM: Even for, you know, end users or home users, you know, have 2 accounts running. Have your own administrator account so if you want to install software or do any kind of administrative tasks on your own system that you use that account, but for everything else, your email checking, your web surfing, your Facebook posting, you use a restricted privilege account. In addition, mobile devices. Now, I said Android is increasingly being targeted. Big problem with Android is that a lot of people will seek out applications from other sources other than the official Google Play Store. A lot of times those apps are malicious in nature, they could be suing your data, especially bank account logins and the like. They could deploy ransomware. Make sure to run antivirus on your Android. Keep that operating system up to date as well as all your applications up to date as well.

JS: That's good advice, thank you again Krista for coming on to the show and discussing ransomware. Hopefully the problem gets less but somehow I figured that once that problem is solved, something else, another whack-a-mole will come up.

KM: Exactly.

JS: You know, the eternal game of cat-and-mouse between security and hacking. So thank you again for coming on to the show, it's always been pleasure.

KM: Alright thank you for having me!

JS: That's it for this week's podcast. Do you have any questions or comments? Feel free to send us an email to podcast@tech.nj.gov For TechNJ, I'm John Silvestri, thanks for listening.