RANSOMWARE: UNDERSTANDING THE THREAT

AND EXPLORING SOLUTIONS

- - -

WEDNESDAY, MAY 18, 2016

United States Senate,

Subcommittee on Crime and Terrorism,

Committee on the Judiciary,

Washington, D.C.

The Subcommittee met, pursuant to notice, at 3:08 p.m., in room SD-226, Dirksen Senate Office Building, Hon. Lindsey Graham, Chairman of the Subcommittee, presiding.

Present: Senators Graham, Whitehouse, and Klobuchar.

OPENING STATEMENT OF HON. LINDSEY GRAHAM, A U.S. SENATOR FROM THE STATE OF SOUTH CAROLINA

Chairman Graham. Thank you. The hearing will come to order, and I apologize for being late. There are more places to be than there are of us.

I am looking forward to this hearing and am excited about the possibilities of dealing with something that is as old as time itself. This is just a different way of shaking people down and stealing. The imagination of the criminal is unlimited, and the counter-response has to be focused and has to balance interests, and that is what we are trying to do here.

I am becoming more aware of it because of Senator

Whitehouse, who is by far, I think, the leading expert in the United States Senate on all things cyber, and I have learned so much from Sheldon, and I am glad we are having this hearing. But ransomware, it can happen to anybody--school districts, hospitals, individuals. And the bottom line is it is the oldest concept out there, shaking you down, taking something that is important to you and holding it hostage, and extracting money from you. And when it comes to systems that hospitals need or school districts need, you are threatening the lives and safety of thousands of people as well as individuals who have to basically have everything maybe in their family stored in their computer, and they cannot have access to it because some crook has locked it down.

It is a terrible crime, and it has its own psychological violent aspect to it, and it is just a matter of time until somebody physically gets hurt because these systems go down.

So our goal here is to understand the depth and breadth of it, to continue to work with Senator Whitehouse to give law enforcement the tools they need. And I was thinking about this today. When it comes to nation states, there are some that are helpful and some that are the problem. We have a state sponsor of terrorism list that the State Department collects, and if you are on that list, bad things

come your way because you are a bad actor.

Maybe what we should think about when it comes to the nation state aspect of it is have a collaboration between the Department of Justice and maybe the State Department and look at the nations out there who are doing a good job in trying to deal with this international problem and find a way to cooperate with them that is mutually beneficial, but identify the nation states that are either turning a blind eye or are actively involved and put them on the bad list to let the world and the American people know who is helping and who is not. I think if you do not wake up some of the nation states where these problems reside in large measure, you are never going to fix this problem. So that is outside of traditional law enforcement. That is a hybrid of law enforcement and diplomacy.

So, with that, I will turn it over to Senator Whitehouse.

Senator Whitehouse. Thank you, Chairman. My first order of business is to ask unanimous consent that a statement and questions for the record from our friend Senator Schumer be put into the record.

Chairman Graham. Without objection.

[The information follows:]

/ SUBCOMMITTEE INSERT

OPENING STATEMENT OF HON. SHELDON WHITEHOUSE, A U.S. SENATOR FROM THE STATE OF RHODE ISLAND

Senator Whitehouse. The second is to express my appreciation to you for holding this hearing and for the work we have done on cybersecurity issues already. We got a law passed to address offshore intrusion and theft of Americans' financial data, which was jurisdictionally foreclosed beforehand, but is a new area of criminal global enterprise, and we were able together to heighten the penalties for trade theft, which is a very common cyber offense. And it is always a pleasure working with you. It is probably going to ruin him in South Carolina, but Senator Graham is one of my absolutely favorite colleagues, and it is a pleasure to do this.

Ransomware has become a real plague on the Internet, on track to inflict $1 billion in U.S. losses this year, according to the FBI. But, obviously, as Senator Graham has said, there is more to this than just the financial loss. An individual whose computer is encrypted faces the loss of very important and sensitive files, legal files, financial documents, their photographs, school records, all sorts of personal things.

Businesses that are attacked by ransomware risk losing their vital business data, business operational mechanisms, and having to figure out how you run while you are under

ransomware attack is a significant problem. And as both South Carolina and Rhode Island have seen, Government entities have to deal with this scourge also. Police departments, fire departments, school districts, and other such entities have battled ransomware and in some cases actually have been forced to make that ransom payment in order to be able to reopen and operate and provide the public the services.

The threat that ransomware poses is perhaps best illustrated by the recent spate of attacks on hospitals. More than a dozen hospitals have been hit by ransomware in 2016 alone, and the danger is not just the ransomware. If you can get into the hospital and shut it down for purposes of ransomware, you can get in there and do that just for purposes of raising hell and risking lives.

The attacks like this block doctors and nurses from accessing the patients' files. They slow down the processing of lab results. In one case, a patient was kept on a powerful antibiotic for more than 8 hours after it should have been stopped because the nurse could not get the lab report because the lab results were delayed as a result of the ransomware attack.

The message from this should also be that we are now at a cyber stage where it is not just breaches any longer. We have jumped from cyber into real space with some of these

things: the attack that Senator Graham is very familiar with in the western Ukraine, attributed to Russian actors that plunged nearly a quarter of a million people into winter darkness.

DOJ--thank you, Mr. Downing, for being here--announced an indictment against Iranian hackers recently who not only attacked dozens of U.S. financial institutions but actually managed to infiltrate the control system for a dam in Rye, New York, which, were it not under maintenance, would have been subject to their control. And this is a warning, I think, to all of us that we need to up our game.

One implement element of upping our game is to go after botnets. Botnets, for those who are not familiar with them, are networks of compromised computers connected over the Internet, often unbeknownst to the owner of the computer, that can be instructed to commit cyber crimes and perform other malicious activities. They are the engine of cyber crime on the Internet, and among other ills, they are closely tied to the ransomware problem that we are going to talk about today.

Senator Graham and I, together with Senator Blumenthal, introduced this week the Botnet Prevention Action, which would empower prosecutors to do more to combat these botnets by: first, expanding DOJ's civil injunction authority to go out and tear down the botnets; two, it would create a new

criminal offense for selling or renting access to botnets--that is a new form of criminal behavior--and then, third, it would raise the penalties for attacks on critical infrastructure computers. I think all that is overdue, and I look forward to working with Senator Graham to get that done.

We have a distinguished panel whom I am delighted to hear from, and as always, Mr. Chairman, I am delighted to work with you on legislation that will give our prosecutors and law enforcement agents the tools they need to stop this cyber threat.

Chairman Graham. Thank you, Senator Whitehouse.

Our first panel member is Mr. Richard Downing, the Acting Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, well known to this Committee and much admired and appreciated. So the floor is yours, Mr. Downing.

STATEMENT OF RICHARD W. DOWNING, ACTING DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. Downing. Thank you very much. Good afternoon, Chairman Graham, Ranking Member Whitehouse. Thank you for the opportunity to discuss the Department of Justice's response to the ransomware threat. I particularly want to thank the Chair and Ranking Member for your continued leadership on the issues of cybersecurity and fighting cyber crime. We truly appreciate your work to ensure that the Department of Justice has the tools and resources necessary to address cyber threats.

The Attorney General has repeatedly made clear that fighting cyber crime is one of the Department's highest priorities. Cyber threats continue to grow more prevalent, more sophisticated, and more destructive. As was described in your opening statements, one threat has been particularly troubling: the rise of ransomware. And because some ransomware variants can infect other computers, a single person opening an email or visiting an infected website can result in the network of an entire organization being held hostage.

The threat of ransomware is staggering. I agree with the statistics that you mentioned earlier, but I would add one more, and that is, one ransomware scheme extorted an

estimated $27 million in just 2 months. And while ransomware fees are typically between $200 and $10,000, victims suffer many additional harms, like the ones you mentioned, quite apart from the pure financial losses.

The growth in ransomware is fueled by many factors. Our computers are still more vulnerable than we would like, and advances in technology, such as anonymizing proxy networks and bitcoin, offer even average criminals highly sophisticated tools to avoid detection.

Despite these challenges, law enforcement is actively working to disrupt and deter ransomware schemes. The FBI currently has dozens of active investigations into different ransomware variants, and this hard work has paid off. In 2014, for example, the Department of Justice led a multi-national effort to disrupt a highly sophisticated ransomware scheme called "Cryptolocker," which had encrypted computer files on more than 260,000 computers.

Defeating ransomware schemes, however, requires a strategy that encourages the public and private sectors to work together. Computer owners everywhere need to improve their digital hygiene by taking steps like installing the latest patches and ensuring that backups are up to date.

The Department has tried to assist in raising awareness by issuing public service announcements about the dangers of ransomware and provide tips on how to protect systems and

respond to malware infections.

In addition, we must work to disrupt the means used to distribute and profit from ransomware. Like other malicious software, ransomware is often facilitated by botnets. As botnets grow more sophisticated and as the threat from botnets continues to evolve, we must continually strive to ensure that our laws remain up to date and provide law enforcement with the tools and authorities it needs to address this threat.

Congress has a significant role to play. The Computer Fraud and Abuse Act, or CFAA, clearly makes it a crime to hack into computers to create a botnet. And, of course, we can prosecute criminals who use botnets to commit other crimes. It is not clear, however, that the CFAA also criminalizes selling or renting access to botnets, which is increasingly among cyber criminals. We support closing this loophole.

In addition, Federal law currently provides courts with authority to issue civil injunctions to disrupt botnets, but only if the botnet is being used to commit certain specific categories of crime. Yet botnets are used for many types of criminal activities such as denial-of-service attacks and sending phising emails. The administration has proposed updating the law to allow courts to issue civil injunctions to stop botnets no matter what the criminals are using them

for, and we certainly are very excited to take a careful look at the bill that has been introduced that addresses these two very problems.

While the use of civil injunctions is a valuable tool, there may be circumstances in which it is preferable to seek a warrant from a court in order to disrupt a botnet. Because of this, the Department supports the Supreme Court's recent action to amend Rule 41 of the Federal Rules of Criminal Procedure to clarify which court agents should go to when applying for warrants in this type of situation. While this amendment would not change the substantive authority to authorize such a warrant, it would reduce inefficiency in the process of applying for warrants of this kind.

With that, thank you for the opportunity to testify today on this important issue, and I look forward to answering your questions. Thank you.

[The prepared statement of Mr. Downing follows:]

Chairman Graham. Well, thank you very much and all your colleagues who are on the front lines of this effort.

When you get a chance to look at our bill, get back with us as quickly as possible, because I think, you know, one, try to make it better; but if you agree with what we are doing, I think your support would help us in terms of getting the legislative process moving more effectively.

Mr. Downing. We would certainly do that, sir.

Chairman Graham. Yes, sir. Senator Whitehouse said about $1 billion is stolen or people are shaken down or extorted, for lack of a better word. What is the potential for this? It seems to be unlimited. If we do not do something more aggressive about it, what can the country anticipate here?

Mr. Downing. It is hard to know where it would all end. The actual instances of reports of it I think are much lower than the actual instances of it actually happening. So when we have tried to look at the figures of the reports that we have received, I think they way understate the actual scope of the harm. And, you know, if we do not do something to try to address the underlying security problems and, frankly, the deterrence that we hope to get among the people who are involved in this, I think $1 billion seems like a low estimate.

Chairman Graham. So it would be a multi-billion-dollar

problem over time if we do not address it.

Mr. Downing. I think that is fair.

Chairman Graham. Has there ever been an effort to prosecute somebody for sort of the residual effects of seizing a computer system? You mentioned the nurse--Senator Whitehouse I think mentioned the nurse delayed for 8 hours. Would you agree with me that if someone did that, they could be held criminally liable, manslaughter, second-degree murder?

Mr. Downing. There certainly may well be State law charges that would apply in those circumstances depending on the intent of the individual. Interestingly, Congress amended the Computer Fraud and Abuse Act about 10 years ago to create very substantial penalties, indeed, life in prison as an opportunity, if there is an intentional attack on a computer system that results in the death of someone. So the penalties could be quite severe.

Chairman Graham. Let us explore that a little bit. Basically, vicarious liability is what we are talking about. So if you are in the business of locking down a hospital computer, that is going to delay treatment, and it makes it harder to administer medicine. Is there anything that we need to do to create more certain vicarious liability? Because I want the criminal to know it is not just the money damages, you know, the money you stole, but it is the lives

you put at risk here. Do we need to do anything different to get to that potential outcome? Because I want to hold somebody criminally liable who puts a student or a patient at risk because of this criminal enterprise.

Mr. Downing. So I think one of the difficulties that you point out in trying to charge someone with a homicide statute is that the defendant could claim, "I just distributed my malware randomly around the world, and I did not have any specific intent to cause harm at this hospital or to this particular individual."

Chairman Graham. But we are talking about crimes that do not require specific intent.

Mr. Downing. True. But I would refer you back to the penalty provisions of the Computer Fraud and Abuse Act, 1030(a)(5) where you damage a computer if it is intentional damage, as this would be, and if you cause death as a result. We actually already have a Federal law in place that would allow up to life in prison for that individual.

Chairman Graham. So in a hospital case, if you did seize the computer system and a patient was delayed treatment and they died, you could have vicarious liability there.

Mr. Downing. I believe so. Yes, sir.

Chairman Graham. Good. So let us open up that front. I want to make it as hard to do this as possible.

Bitcoin--I am by no means an expert on this, but is there anything--the bitcoin aspect makes this crime much more likely. What can we do, if anything, here in the bitcoin arena?

Mr. Downing. That is a good question. Certainly bitcoin, many of the features of bitcoin make it very attractive to criminals. It has got irreversible payments. It has no central oversight. It has a decentralized structure so that it is very hard to trace payments. And so it is really an ideal currency in some ways for the transfer of criminal penalties.

I would have to take back your question, though, on what sort of larger issues or what Congress could do to improve that situation.

Chairman Graham. Well, think outside the box, because if you could make that aspect of this problem more difficult for the criminal, you are making their lives more difficult.

And, finally, when it comes to nation states, are Russia and China a pretty ripe area for this activity?

Mr. Downing. For ransomware in particular?

Chairman Graham. Yes.

Mr. Downing. A lot of the threats for ransomware we have seen coming more out of Eastern Europe than we have out of China. And as far as nation states, we have seen--well, at least for the types of ransomware that we are talking

about, it is more of a criminal motive to date than it has been a sort of political or larger motive than that.

Chairman Graham. Right. I guess the point I am making is that we do have lists for state sponsors of terrorism where the state itself is funding terrorist organizations. It seems to me there are certain nation states who turn their eye or somehow the criminal is connected a bit, you know, to the officials. So what I want to do is put people on notice that we expect you to help the world at large, not just the United States, and create some international standards; and if you are not seriously involved in trying to stop this, that you can be on the bad list in terms of a nation state who is, you know, through indifference or actual aggression, becoming a safe haven for cyber criminals. So I want to make it harder for nation states who look the other way to pay a price.

With that, I will turn it over to Senator Whitehouse.

Senator Whitehouse. Thank you, Chairman.

Mr. Downing, you described the manner by which botnets are vehicles for fraud and criminal activity, specifically including ransomware. There are also botnets that are latent, that it is hard to prove are presently engaged in criminal activity, but with a simple stroke of the keypad could be launched in a criminal enterprise. So what I see is actively engaged botnets that are being used for criminal

activity and latent botnets that are sitting there waiting to be used for criminal activity.

Is there a third category of good and benign botnets that ought to be protected?

Mr. Downing. No. The way we use the word "botnet," it is entirely a criminal enterprise. There is no lawful use for such things.

Senator Whitehouse. I have never heard of a good botnet, and I do not think there is actually a botnet caucus here in the Senate to defend botnets. But in that light, could you explain why the Department supports broader civil authority to allow it to go out and tear down the botnets? What is the distinction that keeps you from doing this all day long just as a hygienic measure?

Mr. Downing. So the current authority that we have used successfully on a couple of different occasions now resides at 18 U.S. Code 1345. It is the ability to seek an injunction to stop ongoing fraud activity. There is also a parallel one for wiretapping.

In those circumstances where the botnet is used to commit fraud because it is, say, stealing banking credentials and people are stealing from banks, that is the circumstance that we can use the current authorities. But there are botnets--

Senator Whitehouse. Well, a latent botnet that is

sitting there waiting to do harm and you concede that there is no such thing as a benign botnet--it is like a weed, and you do no harm uprooting the weeds--that is the problem. You cannot get out there and get them until they are actually hurting people, even though there is no good use for them.

Mr. Downing. That is true. There is a market for the selling or renting of these things, and so some criminals just develop the botnets, have them ready to go, maybe with built-in code, maybe not, because it is very flexible to update the code that is residing on them. There are also some botnets that are used for other purposes like denial-of-service attacks. Those two categories do not fall until 1345, and so we could not at this point seek a civil injunction to stop those--

Senator Whitehouse. Even a botnet that is engaged in a DDOS attack you cannot take down.

Mr. Downing. Correct, not under 1345.

Senator Whitehouse. Okay.

Mr. Downing. Which only applies to fraud.

Senator Whitehouse. Great. Well, we look forward to trying to expand that authority for you, and we are going to try to do it in two ways: first, by opening up the civil injunction authority, and, second, by enhancing your penalties and your ability to get after these guys. So we

are very appreciative of what you are doing.

Tell me just a little bit before I close out here about the issue of trafficking in botnets. Give me a hypothetical scenario that is consistent with the kind of behavior that you see, and noting for the record that this would not be criminal conduct right now because this is a new form of activity that the laws do not reach.

Mr. Downing. So we have had situations where undercover FBI agents or Secret Service agents go on to a forum that is an underground bazaar for the trading of information and capabilities for committing cyber crime. In those circumstances, openly advertised for sale will be, "I have a botnet of 10,000 computers that I am willing to sell you or rent you for X price."

Sometimes the undercover officers go on and say, "Okay. I will buy your botnet from you, and I will arrange to pay you," and maybe it will be bitcoin, and it is hard to identify the person. But say we get to the end of the road and we actually figure out who the person is and we want to put handcuffs on them. At that point the question would be: What is the charge? If the person made the botnet, we could charge that. If the botnet used the botnet to commit fraud, we could charge that. But the mere selling to an undercover agent is not clear that that is a crime at all because you cannot conspire with a Government actor and what crime is it

that he is involved with? That is the sort of nugget there where I think there is a circumstance where we have had trouble and that I expect we will have trouble. We would like to be able to do that sort of case going forward or in situations where perhaps it has not, as you said, been used yet to commit any particular crimes. We would like to see that loophole be closed.

Senator Whitehouse. And is the trafficking in botnet access a fairly widespread phenomenon now? And where do you see it going in the future?

Mr. Downing. It is, unfortunately, common, yes. The problem is that, as we have talked about, botnets are so useful for committing a variety of other sorts of attacks, and now that we have seen so much more ransomware types of attacks, it has become all the more useful for people to be able to rent a botnet so that they can then use it to facilitate a ransomware attack going forward. So we expect this to be one of those things that continues to expand.

Senator Whitehouse. Thank you, Chairman.

Chairman Graham. Senator Klobuchar.

Senator Klobuchar. Well, thank you very much, Mr. Chairman and Senator Whitehouse, for holding this important hearing. And I think sometimes people think they see this crime on, you know, TV shows or in major companies out of New York City. But, in fact, it hits everywhere. My best

example of that is in the Minnesota city of Cloquet, and it is between Minneapolis-St. Paul and Duluth. One day this March, all the school servers went down, affecting everything from emails of students to smart boards and even the school bells in the school. Just a regular Small Town, USA.

Malicious software, in fact, had encrypted the school's computer system, and the perpetrators were more than willing to give the school system the password to unlock the school system's own computers for $6,000, the thing flashed up. So Cloquet refused to be cowed, and they had to cancel school for the day to fix the system, and this was attempted extortion, no different than a classic protection racket. And Cloquet is not alone. Cyber criminals, as you guys have been discussing, are targeting everyone, including police departments, hospitals, businesses, and individuals.

So my first question is really off of that. These guys have no problems flouting the law. You said that you would like to see some legislation passed to close what you call a loophole, so it is very obvious that this is a crime and that we can go after it.

What are some other actions that people, do you think, should be taking besides a legislative action, whether it is on the Government level or on the industry level?

Mr. Downing. That is a great question. I think what

we need to do is really have a two-pronged approach, both the public sector and the private sector. And from our perspective, we are going to very aggressively go after the actors who are behind this. There are a lot of difficulties in doing that, not just needing to pass international borders but also all of the technology that is available to make it more difficult for us to even identify those people. So there are a number of challenges, but the FBI has over two dozen investigations open now, so we are going to aggressively pursue this.

The other half of it, though, is to really make--on the prevention side. People in their own homes but also businesses and security companies need to take steps to try to address to prevent the ability for this malware to get on their machines in the first place. And the average home user can take certain steps like making sure that their software is patched and that their antivirus is up to date, being cautious about emails that they are receiving because they could be phishing emails. But also we can see that from a corporate perspective it is very important for them to have response plans thought through in advance and to think carefully about how to do backups to make sure that if this does befall them, it is going to minimize the damage to their company and their ability to get back on their feet.

Senator Klobuchar. So what are the risks, do you

think, for an individual of having this happen, even if they try their best? And a lot of people are not going to know what to do.

Mr. Downing. Unfortunately, I wish the state of cybersecurity for the home user was better than it was. There certainly are things one can do to try to improve, but, sadly, the best we are going to do is still not going to be perfect, and I think people will be susceptible to this for a while. That is partly why I think we need a two-pronged approach. We are going to have to do everything we can on this side, but we are also going to need a law enforcement response.

Senator Klobuchar. You mentioned that one common delivery mechanism of ransomware is for a party to plant the malware on a legitimate website, which then infects those that visit the website. How can users protect themselves from that kind of an attack?

Mr. Downing. It is very difficult. I think there are two parts to solving that problem. The one side is the user side, which we have talked a little bit about, making sure, for example, that the person's Web browser is as up to date as possible so that it is less vulnerable to that sort of attack.

The other side is to improve security on the website side. Very often, these websites have their own

vulnerabilities which let the criminals get in in order to install their tools that would download the ransomware to the user.

So really it is a two-part cybersecurity problem there on the user side but also on the website side as well.

Senator Klobuchar. All right. Thank you very much, and thanks for your good work.

Mr. Downing. Thank you.

Chairman Graham. Thank you. Just to kind of wrap this up, there are botnets that engage in harmful activities that do not engage in fraudulent activity.

Mr. Downing. Correct.

Chairman Graham. That is what we are trying to address here. Okay. Thank you very much, Mr. Downing.

Mr. Downing. Thank you.

Chairman Graham. Anything else?

Senator Whitehouse. Thank you for your service.

Mr. Downing. Thank you.

Chairman Graham. Would our second panel please come forward?

[Pause.]

Chairman Graham. Thank you all for coming. Our second panel consists of Mr. Charles Hucks, executive director of technology, Horry County Schools, Conway, South Carolina. Thank you for coming.

Mr. Adam Meyers, computer security researcher, Washington, D.C.

And Mr. Charles Blauner, global head of information security, Citibank.

Thank you all very much for attending, and, Mr. Hucks, if you will start us off.

STATEMENT OF CHARLES C. HUCKS, JR., EXECUTIVE DIRECTOR OF TECHNOLOGY, HORRY COUNTY SCHOOLS, CONWAY, SOUTH CAROLINA

Mr. Hucks. Thank you. Chairman Graham, Ranking Member Whitehouse, and other Committee member, thank you for the opportunity to speak to you today on this pressing matter from the perspective of a recent victim of ransomware.

February 8, 2016, started as just another Monday in Horry County Schools. The sun was shining; our 43,000 students and 3,800 faculty and staff were returning for another week of world-class learning and teaching in coastal South Carolina. Little did we know that one of the most disruptive events in recent history was already well underway throughout our district. This event was a malware ransom attack, and it was a big one. We had experienced a few small, isolated infections that were limited to single users or schools in the past, and in those cases, the recovery and restoration was easy and relatively quick, but not this time. This one was different.

After the third school called with reports of encrypted files, the decision was made to shut down all district servers, well over 600, in an attempt to stop the spread of encryption from continuing. It was big, and it was virtually everywhere.

Previous infections were the result of individual users

clicking a link or opening an attachment, typically received via email, that contained malicious code that encrypted any data files found. General user file access is normally limited to team members' home campus so impact was contained. This event was district-wide. At this point it was not known exactly how many systems had been impacted by the attack, but the conditions of the extortion were clearly stated in the ransom note left on every computer infected. All data files claimed to be encrypted with RSA 2048-bit encryption with a different key used for each computer. The price for the keys, payable in the digital currency bitcoin, was 1.5 bitcoin, or around $850 at the time for company computer, or 22 bitcoin, which was around $8,500, for all computers. The note also contained a link for the WordPress site to be used to communicate with the attackers and contain the deadline for payment--1 week.

Once everything was down, careful investigation of systems began. Since the full extent of the infection was not known, each server had to be isolated before powering up for inspection, which is tedious and time-consuming work. While servers were not fully functional, all of the devices issued to our teachers and students, which includes iPads for all students in grades 5 through 8, Dell Windows tablets for all students grades 9 through 12, and an assortment of tablets, desktops, and laptops for all students in other

grades were completely isolated with no ability to communicate with each other or the outside world. Access to email, social and instructional media, online digital content and instruction, collaboration, assessment tools, and network and cloud-based storage was lost.

A report to the Computer Crimes Division of the FBI was created, and the incident was communicated immediately to the local FBI office, SC SLED, SC Department of Education Computer Information Security Office, and the SC State Computer Information Security Office. All asked for continuing reports on progress, any contact with the culprits, and copies of all artifacts from the event, which were provided.

The recommendation to pay the ransom was immediately made by technology to administration and the Board of Education, even before all of the details of the scope of the attack were known. If the encryption was widespread, the rebuilding and restoration of all servers and all end-user data would take weeks, even if the backups were perfect, as it had already been discovered that the attack not only encrypted data files, it also deleted the local operating system backup files which can make restoration quick and relatively painless.

The daily business value of 43,000 students and 3,800 faculty and staff who are unable to access portfolios, class

projects, term papers, lesson plans, and so forth quickly and easily surpassed the $8,500 ransom value.

Forensic analysis of systems impacted indicated the entry point for this attack was through an older application server that was kept in service for access to historical data. Since this application was no longer a production server, updates to the underlying components were not possible, and one of these components contained the vulnerability used to compromise the system from across the Internet and spread throughout the network.

Technology personnel worked around the clock inspecting, rebuilding, and restoring servers in a business priority fashion to return devices and data to all users as soon as possible, with the most core functions restored within the first couple of weeks. The ransom was finally paid, and it was discovered, even when funds are available, the conversion of dollars to bitcoin is not necessarily a simple task and can take quite some time. If not for the assistance of Troy Wilkinson of Axiom Cyber Solutions in Las Vegas, Nevada, who once work in law enforcement in our community and offered to facilitate the exchange for us at no cost, the payment deadline would have never been met.

Needless to say, the event and recovery were a learning experience for all involved. As you would expect, all servers and infrastructure have been reviewed, secured, and

processes improved to reduce the likelihood of a repeat occurrence. Horry County Schools is also involved with the FBI's Infraguard, the State of South Carolina's SCCyber initiative, and ongoing security training.

Thank you for the opportunity to share our experiences and your efforts to provide additional protections for such future events.

[The prepared statement of Mr. Hucks follows:]

Chairman Graham. Thank you.

Mr. Meyers.

STATEMENT OF ADAM MEYERS, COMPUTER SECURITY RESEARCHER, WASHINGTON, D.C.

Mr. Meyers. Good afternoon. I would like to thank Senator Graham and Senator Whitehouse, as well as the members of the Committee, for inviting me to present testimony in today's hearing on ransomware.

I have been involved in the research of cyber adversary activity for well over 15 years. I began my career in the defense industrial base, where I supported numerous federal customers across the Federal Government in information security matters. Since 2011, I have led the intelligence team at CrowdStrike, a commercial security company in Irvine, California.

Ransomware is a scourge, as Senator Whitehouse said. It is software designed with the malicious intention of compelling a victim to pay a monetary ransom in exchange for access to their own data. Modern ransomware originated in the mid-2000s, and the earliest incidents closely mirror what we see today: a victim receives an email containing a payload that, when opened, sets off a chain of events that can ultimately cost the victim irreparable data, memories, and time. Even more terrifying than the email distribution is the use of "exploit kits" that can deliver ransomware to an unsuspecting victim who simply visits a legitimate website that has been compromised by an adversary.

Historically, there have been two primary modes in which ransomware operates: encryption-based and fear-based. The fear-based model attempts to scare victims into paying a ransom under the threat of prosecution for software piracy, possessing pornographic or forbidden material, or simply losing access to their computer. This ransomware, which was far more common at the beginning of this decade, would create a warning to the user of that system, and it would often purport to be from law enforcement. Fear-based ransomware variants have become less common as encryption-based ransomware exploded over the past several years.

Incidents of encryption-based ransomware date back to the mid-2000s. These variants encrypt components of the victim's file system using a variety of cryptographic algorithms, leaving behind a ransom note demanding payment for the decryption of these files. A variant known as "Cryptolocker" kicked off the modern ransomware epidemic in 2013. This variant demanded that the victim pay several hundred dollars, and it would begin incrementing the price of the ransom over time if it was not paid, until ultimately destroying the cryptographic key, preventing access to the data.

Cryptolocker was delivered frequently as a secondary payload from a botnet infrastructure known as Gameover Zeus, which was used to conduct a variety of criminal activities

including the collection of information of intelligence value to the Russian Federation.

In May 2014, in concert with private industry researchers, including several researchers from my team, the international law enforcement community and the U.S. Department of Justice conducted an operation to disrupt both Gameover Zeus and Cryptolocker. The operation was ultimately successful in disrupting Cryptolocker; however, soon copycat variants emerged. Cryptowall quickly rose to prominence, succeeded by a variety of other variants known by names such as TorrentLocker, Teslacrypt, Locky, Cerber, and numerous others.

The distribution of ransomware relies on elements of the criminal ecosystem. Services such as pay-per-install botnets, loaders, exploit kits, spam botnets--all are used to distribute ransomware. The ransomware does not self-propagate; it rides other services in order to reach its target.

The revenue generated by ransomware is not insignificant. This is perhaps the biggest challenge with dissuading attackers from continuing to develop and deploy these threats. Open-source reporting indicates millions of dollars were paid to the actors behind Cryptolocker. Through my team's own research, we observed a niche player who in 3 months made $73,000 from their ransomware campaign,

and they appear to only be getting started. The attraction for attackers to use ransomware is obvious. It provides huge payoffs with little investment.

These attackers have two choices: They can purchase ransomware as a software package, or they can build their own. The sale of ransomware illustrates the breadth of the criminal ecosystem. A relatively novice or unsophisticated actor who finds their way into the right forum can go about buying a ransomware package, enlisting the services of a botherder to distribute their payload and a law enforcement-resistant infrastructure provider to host their command and control systems with relative ease. Once they have employed these services, they simply watch as the money flows in.

Beginning in 2016, a trend emerged that has become quite common: hospitals across the United States and Europe have been locked out of their own data and forced to pay a ransom. This has spread into school districts and even just last week in the House of Representatives. This trend, unfortunately, is not likely to dissipate in the near future. Organizations lack comprehensive protection, fail to ensure that they have adequate backups, and in general do not have any safeguards or countermeasures to stop ransomware from impacting their operations.

Individuals and corporations seeking to protect themselves must maintain adequate backups. Behavior-based

security technology can detect the scanning of files and the encryption of those files, as well as other unique behaviors of that ransomware, which can be used to prevent it from deploying onto the system.

In closing, ransomware continues to be an attractive tool for criminals who seek to terrorize individuals and businesses in order to extort payment in exchange for sensitive data. Ransomware is continuously being developed in order to improve effectiveness, reach, and impact. These tools are distributed amongst a global criminal ecosystem that exists outside the purview of law enforcement. Individuals seeking to protect themselves must remain vigilant and ensure that they make judicious backups of their data. As long as victims continue to pay these ransoms, these malicious actors will continue to be emboldened to operate.

Thank you for the opportunity to testify before you today, and I look forward to your questions and continued discussion.

[The prepared statement of Mr. Meyers follows:]

Chairman Graham. Thank you.

Mr. Blauner.

STATEMENT OF CHARLES BLAUNER, GLOBAL HEAD OF INFORMATION SECURITY, CITIGROUP, INC., WARREN, NEW JERSEY, ON BEHALF OF AMERICAN BANKERS ASSOCIATION

Mr. Blauner. Chairman Graham, Ranking Member Whitehouse, and members of the subcommittee, my name is Charles Blauner. I am a managing director and I am the global head of information security at Citigroup. In this capacity, I set Citi's information security strategy, and I am accountable for overseeing information security risks across all business lines, functions, and regions.

I appreciate the opportunity today to testify at this important hearing representing the American Bankers Association.

I also had the privilege of serving as the Chairman of the Financial Services Sector Coordinating Council from 2012 to 2014. Citi, along with our counterparts in the industry, is extremely supportive of the FSSCC and its sister organization, the Financial Service Information Sharing and Analysis Center. A description of these two groups can be found in my written testimony.

We as an industry have made a concerted effort to work with Federal, State. and local officials in protecting, detecting, and defending ourselves and our customers against cyber attacks. Financial institutions continue to be subject to ever-evolving cybersecurity and other

technological risks. We continue to devote significant resources to maintain and regularly upgrade our systems and our networks.

As the Committee is well aware, the increased illicit cyber activities of nation states and criminal enterprises present a challenge for us as a Nation. A common practice is to utilize botnets, or armies of infected companies and servers distributed globally, to deploy traffic or malicious software, also known as "malware," to perpetrate a denial-of-service attack, to infect our financial customers' electronic devices in order to compromise their personal financial information, to hijack their Internet banking sessions, or to encrypt their important files and then hold these files hostage for ransom, commonly known as "ransomware."

Most recently, we have seen the rapid evolution of what is called "Ransomware as a Service" as malware and ransomware developers offer customized versions of products to other cyber criminals for a percentage of their profits. Ransomware as a Service is likely to result in even greater infection rates as this business model continues to draw new participants.

As bank customers tend to be targets of these attacks, financial institutions, working with law enforcement, have focused on educating our customers on how to protect

themselves.

Customers are encouraged to: make sure they have latest antivirus software; to automate the installation of security patches for operating systems and Web browsers; to create strong and varied passwords; to use pop-up blockers; to download software only from known and trusted sites; and not to open attachments or click on an URL in unsolicited or suspicious emails, even if it appears to be coming from friends and family. These same precautions apply to customer mobile devices as well as desktop environments.

To prevent the loss of essential files due to ransomware infection, law enforcement and financial institutions also recommend that individuals and businesses conduct regular system backups and move those backups offline.

We are also supportive of the action taken by the administration through Executive order authorizing the imposition of sanctions on individuals and entities responsible for malicious cyber-enabled activities.

We also applaud the recent indictments of those Iranians alleged to have attacked the financial services infrastructure in 2012 and 2013.

Through this Committee, Congress took important steps last year to prohibit the sale of Americans' financial information and protect trade secrets.

The Botnet Prevention Act of 2016 adds important provisions to assist prosecutors in stopping criminals and foreign agents from leveraging botnets; enhances the Justice Department's ability to deter the criminal use of botnets; imposes tougher penalties for damage to critical infrastructure computers; and targets the trafficking of access to compromised computers within a botnet.

We as an industry look forward to working with Congress, this Committee, and the administration to improve the tools necessary to deter, detect, apprehend, and prosecute those that use technology for criminal purposes.

Thank you for holding this hearing, and I am happy to answer any questions on this important matter.

[The prepared statement of Mr. Blauner follows:]

Chairman Graham. Senator Whitehouse.

Senator Whitehouse. Thank you, Chairman.

Mr. Hucks, welcome. I can remember Senator Graham mentioning the incident that you sustained, and now here you are and we are having a hearing. I appreciate that you took the trouble to come up.

I also appreciate the attachment to your testimony, which I do not know if people who do not have it in front of them would have any way of knowing this, so for the record, this is a copy of the ransom note that was left on the computers with instructions as to how to clear the ransomware, and at the end, it says, "Check our blog. We generated a decryption software for your computer randomly. Don't worry, it's not malicious software." Who are you going to believe about what is not malicious software more than the guy who just hacked you and ransomed your system? Really something.

Did you get advice in your circumstance from local law enforcement as to whether or not to pay the ransom?

Mr. Hucks. Law enforcement was very hesitant, whether that be local law enforcement, FBI, SLED, even the State and State Department of Education computer security officers were, of course, very forthcoming in saying that they were philosophically opposed to paying the ransom, but they understood that there are situations where we may choose to

pay. So the official response of all involved was, "We do not condone this, but we understand if you do."

Senator Whitehouse. Yes, understood.

Mr. Meyers, you have talked about the prevalence of these botnets. You have talked about the Department of Justice's work taking down Cryptolocker and taking down some of the--or addressing Cryptolocker and taking down some of the botnets. In your view, if the Department of Justice were empowered to go after botnets, had broader authority to take them down, would there be business for them? How large is the scope of the work of tearing down the botnets that now infest the Internet?

Mr. Meyers. Yeah, I believe that they would have quite a bit of work in front of them. There is no shortage of--

Senator Whitehouse. Is that understatement?

Mr. Meyers. There is no shortage of botnets that are ripe for disruption, and I think that that comes with, you know, having the ability to do that disruption and also the partnership with private industry to help facilitate the actions of the Department of Justice, because it is not just a problem for them to solve. I think it is a problem for the broader community to solve and work together to figure out how to disrupt those botnets.

Senator Whitehouse. I think the witnesses, including our Department of Justice witness, have all spoken of

ransomware, of botnets, and of bitcoin. Give us just the overview of how those three link together.

Mr. Meyers. Sure. So the connection, I like to think of it as an ecosystem of criminal capabilities. So while one botherder might stand up a botnet, they will make that accessible to anybody that wants to pay to use it. So they will go out and infect hundreds of thousands of machines, and then when the ransom--

Senator Whitehouse. Often using a broker, an intermediary, to--

Mr. Meyers. Sure, yes, so an exploit kit or a spam botnet. So these things all get chained together. So perhaps the loader gets distributed by spam, and they pay a spam botnet to distribute their spam template, which then proceeds to install that loader.

Once that loader is in place, then they can sell access to the highest bidder. If that be a ransomware actor, then they will be able to pay that loader to distribute that ransomware behind the scenes. And once it is installed and that ransom is paid, then they are able to collect that fund in bitcoin.

Senator Whitehouse. And bitcoin protects the identity of the payee and helps them hide from what they have done.

Mr. Meyers. Yeah, it makes it much easier to collect that fund. There is really no oversight over how bitcoin--

there is not a lot of taxing or things like that that they have to pay for. So--

Senator Whitehouse. And the criminal can retain their anonymity with bitcoin.

Mr. Meyers. That is right. Absolutely. It is peer-to-peer cryptocurrency.

Senator Whitehouse. So somebody who gets a ransomware signal on their computer and it is locked down has not necessarily been targeted individually by somebody who has gone after that computer. What they have done is they have launched the ransomware across botnets, and wherever it lands and sticks, they have a potential victim, and then the victim, paying through bitcoin, can bring it back in ways that are relatively secure from a point of view of the criminal enterprise.

Mr. Meyers. That is right. It is opportunistic. And I have seen that there are numbers around the 40 percent of people that actually pay that ransom. So if you figure--you know, you can do the math behind that.

Senator Whitehouse. That is a high hit rate.

Mr. Meyers. Yeah.

Senator Whitehouse. Very well. My time is up, Mr. Chairman.

Chairman Graham. Thank you.

Mr. Hucks, let us continue in that thought process.

Why did you pay?

Mr. Hucks. Very early in the event, we realized that this was quite a widespread event. We have, as I mentioned, over 600 servers. These servers are spread across our 52 campuses where at each of those campuses we have file servers that store the files and the work of all of our students and all of our faculty.

Once it became clear that a large majority of this data had been encrypted, the backup scenarios that we use, we primarily centralize our backups at our district office and our data--

Chairman Graham. Is it fair to say you had no choice?

Mr. Hucks. We had no choice if we wanted the data returned in a reasonable amount of time. So certainly with any backup scheme, there are holes in your backups. You may not back up everything. But even if you do, the amount of time to restore it can be significant. So we felt the business value of getting that data back in the hands of our students and our teachers was worth the $8,500 ransom to expedite that restoration of data.

Chairman Graham. And when it comes to law enforcement, they could not assure you that they could fix this problem anytime soon.

Mr. Hucks. Not at all. Not at all. They said, "Good luck, and please keep us posted." They asked us to provide

as much data as we could on any communication that took place between us and the attackers so that they would have more data to try to track down exactly where the attack originated. And we certainly did that.

We have heard since then and around the time of the attack that there were numerous organizations that were hit through the same vulnerability that we were that the FBI was tracking.

Chairman Graham. Did they have any clue who did this and where they were operating from?

Mr. Hucks. No, sir. If they did, that was not shared with us.

Chairman Graham. Okay. Just very briefly, what kind of disturbance did it cause for you? Was this a fairly traumatic event for the school district?

Mr. Hucks. Well, I have been working in this field for 30 years, and it was probably the worst month of my life. So it was rather significant. The first day, Day 0 of the event, all of our computing resources in the entire district were shut down, and this is a district where there is daily dependence on the use of technology. All of our students grades 5 through 12 have a personalized device that is issued to them by the district that they use all day, and it was essentially a stand-alone device for that first day.

We were able to restore Internet and network activity

on the second day, and in the days that followed, we were able to restore the operational systems on a priority basis. But a full restore of all capabilities and all systems took a matter of weeks.

Chairman Graham. Thank you.

Mr. Blauner, have you looked at our legislative proposal?

Mr. Blauner. I have not reviewed the proposal at this point.

Chairman Graham. Would you please review it and get back with us on trying to make it better?

Mr. Blauner. Yeah, absolutely.

Chairman Graham. Do you generally believe the Committee has been on the right track with what we have been trying to do in terms of dealing with this issue holistically?

Mr. Blauner. Yeah, I think we as an industry are very supportive of the idea of making this game more dangerous from the criminal hacker.

Chairman Graham. That is my goal. That is my goal, is to make the upside a lot greater--I mean, downside a lot greater than the upside. That is the goal. And whatever we need to do to make the downside greater is what I want to do, understanding we are Nation of laws.

Where do you see this crime going if we do not up our

game, as Senator Whitehouse talks about?

Mr. Blauner. I think we as an industry view this as an accelerating problem. Financial services especially has always been a target. It goes back to when criminals actually had to physically go somewhere. But the reality is back in the old days, the odds were sort of in our favor. The risk-weighted return on investment for a criminal was very low. The risk-weight return on investment for a criminal now is very high, and their cost gets cheaper and cheaper as they no longer have to be technical experts. They can buy the services necessary, and, thus, the cost of entry for a criminal is marginal. And, thus, for them, until we make it more painful, it will continue to accelerate.

Chairman Graham. The worst is yet to come.

Mr. Blauner. Yes, without intervention.

Chairman Graham. As you can tell from Mr. Hucks' testimony, this can be a very devastating event.

Mr. Meyers, quickly here, tell me about what can we do when it comes to the bitcoin world as a legislative body? And how do we do what the gentleman just said, make the downside greater?

Mr. Meyers. In terms of making the downside greater, I think we need to really focus on where it is more expensive for these adversaries to operate. If we are able to raise

the cost of doing business, whether it be getting onto a machine or whatever it might be, if there is a way to kind of turn the table in the economic model there and make it more expensive for them to operate, that is when we are able to make that downside.

Chairman Graham. What about nation state collaboration? Are there nation states out there that are actively involved in this kind of activity?

Mr. Meyers. Yes, I believe there are.

Chairman Graham. Do you agree with that, Charles?

Mr. Blauner. Our observation is that there are nation states that do not necessarily cooperate well with the FBI as you try to chase a criminal down.

Chairman Graham. So botnet havens, for lack of a better word?

Mr. Blauner. I think it is more about havens for the human beings. The botnets can be anywhere.

Chairman Graham. Anywhere, yes.

Mr. Blauner. It is not the computers that are doing the harm. It is a set of human beings behind them.

Chairman Graham. A place where they know the upside is--the downside is pretty low.

Mr. Blauner. A place where they know that prosecution and extradition is unlikely.

Chairman Graham. Okay.

Mr. Meyers. I would say that in many cases you will see that the malware will actually look to see if the keyboard or the language that is used on the machine that is being affected is Russian and will not infect it in those cases.

Chairman Graham. Briefly, name a couple of countries who you think are the worst offenders.

Mr. Meyers. I would probably start with Russia, and the list would be various Eastern bloc countries behind that.

Chairman Graham. Do you agree with that, Mr. Blauner?

Mr. Blauner. I think I would leave attribution to the law enforcement agencies.

Chairman Graham. All right. Thank you all very, very much.

Senator Whitehouse. Another question?

Chairman Graham. Yes, absolutely.

Senator Whitehouse. First of all, I wanted to offer Mr. Hucks a little bit of reassurance. If it is any consolation, it is one thing for a school district to be hacked this way. When a school department happens, it is a pain in the neck, but, you know, it is what it is. It has happened to police departments. If you are police department who has gotten shut down by this, there is a whole extra layer of embarrassment and frustration. So I am

not saying that it could not be worse, but I really much appreciate you coming here.

And I just wanted to ask you, Mr. Meyers, to repeat what you just said. There are malware programs that have baked into their programming the capacity to read the computer that is being infiltrated, and if it sees Russian language, to stop?

Mr. Meyers. That is correct.

Senator Whitehouse. Gee, I wonder who would want that.

Chairman Graham. I have no idea. We are going to make Russia great again, I guess.

[Laughter.]

Chairman Graham. So the bottom line is this has been very helpful, and we want to make the downside so much greater than it is today. And if it were not for Senator Whitehouse, I would know zero about this. I am not a computer expert by any means. But he has opened my eyes, and I hope through this process we can open the eyes of--

Senator Whitehouse. Just like the guy at the poker table, he is looking over and saying, "Now, remind me again. Three of a kind or two pair, which one wins?"

Chairman Graham. I have got a flip phone. I can back up. I do not know a whole lot.

[Laughter.]

Chairman Graham. But the bottom line is this seems to

be ripe for exploitation. I can see terrorists getting involved. The amount of money that could be stolen this way--like you say, the hit rate is 40 percent. That is pretty darn good. And so I just want to keep working with you. You are really smart on this, and I want to do everything we can in a bipartisan fashion to get to it.

Senator Whitehouse. And, Mr. Blauner, your testimony on page 9 says that the American Bankers Association fully supports the goals of our Botnet Prevention Act of 2016, but I detected some hesitancy from you just now.

Mr. Blauner. Oh, no. I think we absolutely support the goals. I was only hesitant on naming countries.

Senator Whitehouse. Okay.

Chairman Graham. Yeah, I do not blame you.

Senator Whitehouse. So you describe our bill. You supported the International Cyber Crime Prevention Act, the original one. We got two pieces of it passed already. These are the remaining three pieces. They are in the Botnet Prevention Act you mentioned and support all three, and the American Bankers Association is on board.

Mr. Blauner. That is correct.

Senator Whitehouse. Great. I just wanted to clarify that.

Chairman Graham. Let us close it out on a positive note. Mr. Hucks, could they have changed my grades?

Mr. Hucks. Well, given the depth of their connectivity to the entire network, they generally could have done anything they wanted. So, yes, they could.

Chairman Graham. Well, okay. I do not know if they were in Russian or not, but, finally, bitcoin, Mr. Meyers, what do we do about this whole bitcoin?

Mr. Meyers. I do not have any idea. I think that is probably better for the Treasury Department than me.

Chairman Graham. Well, thank you all. This has been very informative. Thank you very much.

Senator Whitehouse. Thank you very much.

Chairman Graham. The hearing is adjourned. Thank you.

[Whereupon, at 4:11 p.m., the Subcommittee was adjourned.]

C O N T E N T S