Ransomware: Best Practices for Prevention and Response

featuring Alex Volynkin and Angela Horneman as Interviewed by Suzanne Miller

---

Suzanne Miller: Welcome to the SEI Podcast Series, a production of Carnegie Mellon University's Software Engineering Institute. The SEI is a federally-funded research and development center, operated by Carnegie Mellon University, and sponsored by the U.S. Department of Defense. A copy of today's podcast will be available on the SEI website at sei.cmu.edu/podcasts.

My name is Suzanne Miller. I am a principal researcher here at the SEI. Today, I am very pleased to introduce to you two colleagues from our CERT Division, Alex Volynkin and Angela Horneman. Both of them have been working in ransomware, which is our topic for today. But before we get to that, I want to talk to each of you a little bit about what brought you to the SEI. What is it that you are doing that is exciting to you about the SEI?

Alex Volynkin: I started my research in information security and computer security with my master's and Ph.D. work in malware analysis. Malware would be the malicious software, which has been a problem for quite a while now. Traditional methods of detection were to apply signature-based approaches to detect previously known malware but not new malware.

In my work, I did research that would dynamically detect malicious software as it executes in the more heuristic approaches, approaches that do not require previous knowledge about that malware. That was my Ph.D. work when I was in grad school.

Later, I was working for industry for a number of years, working on cryptographic solutions. That would be for payment systems, for a variety of data protection solutions, encryption solutions, and things like that. Later, I came to the SEI, and here I work as a senior research scientist. My areas of expertise vary from malicious software analysis to cryptographic solutions and analysis of security of cryptographic solutions and also hardware and network security.

Suzanne: Angela, what brought you here?

Angela Horneman: I went back for my master's after spending several years in industry. I was not feeling that there was much room for growth in what I was doing, which was a little bit of everything for a mortgage software company. I decided that security seems a lot more interesting and I can make a positive impact. Where, when you are working with mortgage software, sometimes you wonder if you are making a positive impact or not. I interned here, starting after the first semester for my master's, and really liked what I was doing and stayed on afterwards.

Suzanne: Both of you have been working recently in this idea of ransomware, which is when, I think most people know, you are being held hostage essentially. Someone gets into your computer and asks you for money or asks you for you something in return for releasing your computer to them. That is kind of a scary thing. This is something that has been increasing.

There was a report in 2017 by Verizon that warned that these kinds of attacks were growing by 50 percent in the last year. Even today, as we are recording this, there is a ransomware attack that people may be reading about in the newspaper that is going on over in Europe. This is a problem that has been around for a while, it is not going away.

The big question is: How did we get to this point? And how do we deal with it? So why do not we start with, how did we get here? How did how did ransomware become such a prevalent aspect of what we have to deal with in today's information security environment?

Angela: I think it [ransomware] is a natural extension of malware. So, it is simpler than stealing. If you are stealing somebody's credit card, then you have to make sure that whatever you are getting, you can cash in on. Whereas if you hold something hostage and expect a payment, well, somebody pays you. It is already there. You do not have to worry about being traced back, the credit card being turned off. You get that money in your account, and you can take it out.

It has been happening for years. Several years ago, you heard about the FBI splash pages that people would get from infected ads or clicking on emails. Well, now instead of just doing a splash page where they access anything else, they are actually encrypting, sometimes individual files, sometimes the whole computer. Occasionally you still do see the splash screens where nothing is really in the background, but it is also becoming more commoditized.

Suzanne: So it is a commodity, so I can actually hire people or hire someone to...

Angela: Yes, there is open source. It is an open source out there. There is ransomware as a service, which you might see as RaaS, where...

Suzanne: Never thought we would see that day.

Angela: Somebody has the ability to conduct an attack, you have somebody you want to attack, you provide them the information, then you split the profits. A lot of places, if you can get a few

home users to pay the ransom at a few hundred dollars each, or if you can get an organization to pay a few thousand dollars for a lot of people everywhere in the world, that is a huge amount of income.

Suzanne: Actually that is I think a good point about this is that it may be outside of the U.S., especially with the open source. The accessibility of this to people that do not have good income possibilities in regular ways. This is actually a fairly cheap way for them to actually make money that is meaningful to them, even though it may not in our economy be as meaningful. So this is not going to go away.

Angela: No, it is not going to go away.

Suzanne: Is really the answer there. So if you are attacked, what do you do? Who you talk to? Who you going to call? We do not have ransomware busters yet. What is a reasonable way to deal with this? So, there are two sides to this. As an individual, what should you do? But also from the viewpoint of us an SEI, as an institute researching this, what are we doing to try and help people avoid this, prepare for it, and recover from it?

Angela: For an individual user, it is a lot more difficult, especially if you are talking about somebody who does not have lot of computer background. They are not really sure how their computer actually works. That is a lot harder for them even to understand how they got infected. Most of the cases that is usually through email. Somebody got an email or did a web search for something that they probably should not have been searching for to begin with, clicked on an ad or something.

Suzanne: We call that clickbait.

Angela: Clickbait. Got installed that way. For many of the ransomware, there may be unencryptors that hackers, the attackers, have made mistakes, so you can recover from it to an extent. Your best option as an individual user may be to contact some reputable support company or a family member or friend. As much as we as security people joke about, everybody is asking us the questions. *Hey, we are here we do know [how to help]*.

Suzanne: I have a brother who is in security, he is the guy I would call. If you have a friend that is reputable in that arena, and knowledgeable, then that can be helpful.

Angela: As an individual user, that is probably your best option, is to find somebody who has some idea what they are doing that you can ask and get their expert advice on.

As an organization, hopefully you have done stuff like backup. That is good for individual users, too. Make sure that you have anything that you have backed up on flash drives or CDs that you do not keep plugged into your computer, because those could end up encrypted if they are

attached. That way you can just take it somewhere, have it reset, wiped, and then just put your important stuff back on.

The same thing goes for organizations. Really they should make sure that they have good backups, but that is a more mitigation after you're infected.

There is a lot that you can do to help prevent it, but it is not perfect. One of the things is be very careful with the email that you get. Really make sure that it is coming from the person who you think it is coming from.

As an individual user, you will see a lot of email from people who you know who are in your address book, but they may have been compromised. I see that all the time where I have several friends whose addresses are spoofed and sent to me all the time, but I know that, *OK, this is just weird. They wouldn't be saying that. Or why would they...*

Suzanne: It is uncharacteristic.

Angela: It is uncharacteristic, or it may be characteristic but there is no background context. *You have not been talking to them about that such that it is something that they would actually be talking to you about through email*. That is probably the biggest thing you should do, is be very, very careful about your email.

Make sure that whatever email provider you have does good spam filtering. The same thing goes for an organization. Be very diligent with your spam filters in your emails. If possible, you know, use text-based email or at least disable any macros and executables from being delivered or executed.

Suzanne: Anything to add to that, Alex?

Alex: Yes, I think I agree with Angela on the preventative measures. One of the biggest things that any organization and individual can do is to back up the data. Because ultimately, if you have the data that is encrypted by ransomware, and you would like to avoid paying the ransom, your easiest way out of the situation is to take the backup that you recently stored away and put the data back on your system.

It will take some time to do the process, but if it is done properly, it should completely, 100 percent, recover what you have lost. This is probably the best preventative measure that can be done with regards to ransomware. Also, it works regardless of the method that the ransomware chooses to encrypt, steal, or somehow prevent you from accessing your data.

Phishing emails has been the primary attack vector to get ransomware on the system. The combination of phishing emails and some sort of exploit that would allow the code that is delivered through the phishing email to execute on the system.

So, making sure that your operating system, all of your software, is regularly updated, all the patches applied to it regularly. And making sure that phishing emails do not get the effect that they are looking for in terms of people clicking on links, executing, downloading, things that they should not be doing.

Suzanne: I know, our own IT shop—I do not know that all email does this, but I think it is a really good thing is—when I see that it is from Angela, it shows me the actual email address that sent it. Well, Angela should have a *sei.cmu.edu* address. If it says Angela in the name, but it has another address, then I know that that is likely to be a phishing email. So, things like adding transparency so that as a user I can actually look at, *What's the source of this?* not just what the name is on it. That has helped me.

We have a special email called *suspicious* that we can send things to so that they can improve their spam filter. There is a user aspect to this of being aware of the possibility that you would be attacked at any time and being cognizant of your environment. It is just like walking down a dark alley, right? You need to be looking at your environment all the time and evaluating, *What is the risk here?* and not just taking for granted that every email is going to be coming from where you think it is.

Alex: That is right.

Suzanne: From the viewpoint of the SEI, what kinds of research are we doing to try and help with improving prevention activities or improving recovery activities?

Alex: We are working on different fronts with regards to ransomware and malware in general, with the ransomware being a subset of malicious software. One of them is early detection. You should be able to detect activities that ransomware is known for before it gets too late, and the user is already infected, and the data is already encrypted.

If we can create some early warnings, either on the network filters, on the spam filters, or actually in the actual computer systems and workstations, or on servers where this is actually useful and actionable. This goes with regards to network filtering. It goes with email filtering as I mentioned.

On the other hand, the other important aspect is educating users about these attacks and the kind of attacks that exist, and what should be or can be done to prevent these attacks. Also, what to do in case this attack has already occurred and how to deal...

Suzanne: Who to report it to.

Alex: How to deal with this. We make sure that we evaluate all of the previously known attempts to install and execute malicious software, ransomware. We basically educate users on the best practices on how to deal with malware.

Suzanne: Do we have some examples of … I gave a pretty intuitive best practice, which is look beyond the name to what is the actual address. Are there some other best practices that are maybe less intuitive that you have been educating IT security professionals, network administrators, about things to watch for?

Angela: The best practices for ransomware are just the same as for other malware. The difference is a lot of the mitigation. Obviously, you have encrypted traffic with ransomware, which you do not with a lot of the other malware. But the same best practices apply: limit admin privileges. Even if you have admin privilege on a machine, do not use it for everyday work because that gives any process running under that account the ability to access everything on the machine. If you can, limit where read and writes can occur.

If you have network attached storage, like if you have a file share, take pains to make sure that those require logins so that they are not encrypted if an individual user is infected. Do web filtering. Blacklists are not very effective. If you can implement whitelisting though, to limit the applications that can be executed on a machine, that is very good.

Suzanne: So that is what whitelisting does?

Angela: Right, do whitelisting. If you have user directories that are meant for data, do not let executables execute there.

Suzanne: So, those are typical of the kinds of things we see in best practices. So that is the good news, right?

Angela: Yes, so, the good news is if you are doing good for malware in general, you should be covered with ransomware. The problem is how you mitigate it.

Suzanne: And the bad news is that the mitigations on this are, essentially, there is one mitigation: wipe it out and replace, which makes that data backup probably the most important mitigation. My 87-year-old father will be glad to hear that because he has literally a desktop full of hard disks that back up his data going back about 20 years. So he is covered, and they are not attached.

Alex: That is actually great, exactly. Because one of the things about backups, and something that we have seen in enterprise environments in the past as well, where there would be backups

and there would be plans to back up the data on a regular basis. And the backups would be executed, but, number one, there would not be a mechanism that would verify that these backups are still valid. So you may still have a stack of tapes or drives, but they may not actually be working and may or may not actually contain the data anymore, given that they may be old or whatever there is…

Suzanne: I am betting a couple of my dad's hard drives fit into that category.

Angela: Or, the fact they are the wrong drives to begin with.

Suzanne: Oh, no, he would never do that.

Alex: Or, on the other hand, you would have the data that is backed up perfectly fine, but it is also network accessible. Newer versions of ransomware seem to be targeting not just your storage of data on your documents, folders, and things like this, but also go after backups, database backups, and so on, either on the personal computers or on the network storage and other storage devices. It is important to have this, what we call, air gap between the network that is currently running and the database backup that needs to exist elsewhere.

Suzanne: That is where my dad is good, because he has got plenty of air gaps. But I am not so sure he is good on making sure that these are all still valid. But, hey, storage is cheap, right?

Those are a few things. I am very happy about the fact that regular practices are part of this, but I am also interested in, *What do you think we are going to see next?*

We started with the malware. We started with the splash pages, the phishing emails. You could always tell it is the beginning of the school season because every new programmer is trying to figure how many people he can touch with his malware kinds of things.

But ransomware, OK, we are getting into some creative and a little too-easy-for-my-taste ways of getting at people. What do we have to look forward to? What should be we be looking for next in relationship to how these kinds of malware attacks are likely to evolve?

Alex: What we have seen so far over the past maybe three, four years that ransomware has been out there and constantly evolving, is that ransomware has been actively catching up with the industry, actually best practices, in terms of how to encrypt the data.

If we look back at the history of ransomware about two, three years ago, they would attempt to encrypt the data, but they would be using broken protocols. They would be using insecure methods to encrypt the data, and therefore, the data was easily recoverable.

As we look at the progression of ransomware now, we see that they are getting closer and closer to what an industry-standard best practice approach to encrypt the data would be. Things that you would see at online banking, at payment systems, etc., where complicated robust encryption solutions are being created.

This is where ransomware is moving to, because they have seen in the past where broken ransomware software methods would cause people to find ways to decrypt the data without paying. Looking back at that, what I think we are going to see in the next two, three years is the methods to encrypt the data would evolve further to make sure that the data is harder and harder to decrypt, which, again, makes the preventative measures probably more and more important. Because, again, the data backup is going to solve the problem regardless of how sophisticated the ransomware is going to get.

On the other hand, ransomware is also moving towards using, again, what we call command-and-control servers more and more in that regard where the encryption keys and the decryption solutions are stored away from access to the user. So, it is in the hands of the attacker at all times and it also makes ransomware more efficient and more deadly, so to speak, in terms of users not being able to recover the data without paying the ransom.

Suzanne: I am also thinking the Internet of things also makes this a little bit…I am seeing that as a potential future. I have heard of some examples of this where it is not taking over your computer, it is taking over some aspect of a water treatment system and things like that. Where it is actually hardware that they are controlling, that has some negative effect if it does not work correctly.

Angela: I think we are going to see that more and more. That, and we will probably also see a rise in not just the fact that they are encrypting, but the ransomware along the lines of, *They are stealing the data that you do not want released, so they are demanding ransom to pay it so they do not release it.* That is going to be very applicable with the Internet of things where you have movie cameras everywhere or you have recording devices. You do not necessarily want everybody to see that.

Suzanne: I do wonder, though, the digital natives that grew up with technology seem to have, in many cases, less of a sense of privacy than people of my age that grew up without technology. I know I have nephews and nieces that, *Yes, go ahead and post all of that stuff. I don't care*.

There do seem to be some different attitudes. There are the possibilities that even though the sophistication increases, that some of the effects may not be what they want if they target the wrong audience. That could be a positive side to some of the changes in the way that privacy is seen by different generations. We will have to see how that evolves.

Alex: Yes, that is true. At the same time, these, I think, create opportunities for tags that involve phishing emails and so on to proliferate because people get to be more trusting and there is more information about them that is available that can be put in a phishing email, especially if it is a targeted phishing email to an organization or to a particular sets of individuals.

Like if you were to receive an email from Bank of America saying that you need to log into your account to verify your credentials, or whatever. And if it happens that people know that you actually have a Bank of America account, you are much more vulnerable to actually clicking on that link and causing trouble if they know that you have a bank.

Suzanne: They put the logo on, and they make it look...except that they have that address that is not from Bank of America. That is how I get them.

Alex: Right, also, what made ransomware very efficient over the past few years is the availability of cryptocurrency. Because previously, it would have been harder to demand payments if these payments were done with money that is traceable. Now, with the availability of bitcoin and similar cryptocurrency, the situation is that you can easily demand money from anyone to pay into an unknown wallet, and it will be hard for law enforcement to trace it back to the attacker.

Suzanne: And it is global.

Alex: And it is global as well, exactly. It can be done from overseas. It can cross boundaries easily. Again, looking into what is going to happen next, use of cryptocurrency is going to probably make it easier and easier, especially now that cryptocurrency seems to be picking up speed and seems to be more and more available.

What is interesting is we have done some research with ransomware that, despite the fact that cryptocurrency was somewhat cumbersome and difficult to use, people still were so motivated to get their data back that they would go through hurdles of acquiring bitcoin through various means--gift cards or prepaid cards, whatever. They would still find a way to pay the ransom to get their data decrypted, and that shows the motivation to get the data. That shows the reason why ransomware seems to be successful.

The FBI reported that during last year, the ransomware payments, just for the quarter of a year, were approaching about $200 million that they have estimated. It is hard to tell, but they have estimated that that is about where we are, right? You can extrapolate that over a few months, you can see that it can easily get into a billion-dollar industry.

Suzanne Miller: Which gives the motivation for people that want to find easy money. This is an avenue that has had some success. So really the message here is, as users, we have to take

responsibility for doing what we can to make sure that if we do get hit with this, we can recover from it. I mean, it is the resiliency thing, right?

I do not know if I am ever going to get hit by this, but if I do, if I am not ready to recover from it, then I am at risk, probably in ways I do not want to be at risk. That is really the message here, is prevent the risk. You cannot prevent it from occurring, but you can prevent the impact. That is where all these techniques come in and these best practices come in.

I think you guys are going to be busy. I am not sure this is what I want you to be busy with, but that is our world right now. So, we need to be aware of this. That is one of the reasons we have this series, is to help people understand what their options are, how they can respond to these kinds of things when it does happen, if it happens.

Alex and Angela, I want to thank you for joining me today and talking about ransomware. I know that you co-authored a blog post on this with another of our colleagues, Jose Morales. That blog post is available on our insights.sei.cmu.edu website. Click on the author tab and go for one of the author last names. Volynkin is a good one, V-O-L-Y-N-K-I-N, and you should be able to find that blog post.

This is one in a series of *Best Practices in Network Security* podcasts. We will provide resources in the transcript that will give you the links to all of the podcasts that we have done so far and ones that are upcoming as well.

For our listeners, places that you can find this podcast included on the SEI website, sei.cmu.edu/podcasts. You can also find it on our on Carnegie Mellon University's iTunes U site. And you can find it on the SEI YouTube channel. Any of those will get you access to this. Thank you for joining us today. If you have any other questions, please don't hesitate to email us at info@sei.cmu.edu. Thank you for watching.