Ransomare: Evolution, Rise, and Response

Featuring Marisa Midler and Tim Shimeall as Interviewed by Suzanne Miller

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

Suzanne Miller: Hello my name is Suzanne Miller. I am a principal researcher here at the Software Engineering Institute. Today I am joined by Marisa Midler and Tim Shimeall, both analysts within the SEI's CERT Division. Today, we are here to discuss their latest work in ransomware, which we have seen a spike in over the last year, both in the number of ransomware cases and their severity. They will explain what ransomware is, if you have not heard about it yet, and also some of the reasons why this may be happening now, and things you can do about avoiding ransomware in your future.

So, I want to welcome both Marisa and Tim. Thank you for joining us today.

Marisa Midler: Hi, thanks, Suzanne. Like Suzanne said, I am an analyst for the SEI's CERT Division in the Situational Awareness Team.

Tim Shimeall: Yes, and I am also an analyst at the CERT Situational Awareness Team here at the Software Engineering Institute. Ransomware, in general, is malicious software that is geared to extort funds from a victim organization. So, classically, what it does is, once it connects to your system, it encrypts data, and then says, *Pay or we will not give you the decryption key*. And there has been some more recent evolution in that threat that we will talk about as we go through the podcast.

Suzanne: Yes, some really interesting things. Before we get into that, why don't you tell our audience a little bit about yourselves and the work you do here at the SEI and what is it that led you down this path to actually be studying ransomware in the current situation? Marisa, why don't we start with you.

Marisa: OK, well, I am actually newer to SEI. I have been here for a little over a year now. And I have worked on a wide assortment of projects, ransomware being one of them. My background before the SEI, I was a software engineer. I still get to do some software development projects here. But I also do operations and virtualization projects, and I have also done some IOS security research.

Tim: I have been at the SEI just a little bit longer than Marisa. I started in April of '99. I have done a number of different projects for the SEI during that time period as you might expect including some of the situational awareness software that we use on a day-by-day basis to analyze network traffic and deal with stuff. Network traffic was where the Situational Awareness Team started, but we go beyond that. We look at malware and malware characterization, such as we are discussing in this podcast. We also look at technique development and coming up with new ways to inform decision-makers about the state of the network or the threats against the network. We have also done a variety of data analysis and data publication to keep people informed about what is possible in the modern networking environment.

Marisa: We have also done some stuff with training, and we have developed workflows to standardize analysts' methods of going through and working through the different problems.

Suzanne: So, a lot of different activity related to networks and situational awareness. I think that frame of situational awareness is really one that our viewers want to be aware of, that the SEI is not just looking at one aspect of malware. We are looking at lots of different aspects, so that when something new, like some of the ransomware things we are going to talk about comes about, SEI is a source for information about that.

Tim: Yes, and the SEI also has a couple of other teams that actively work in related spaces to this. There is the Vulnerability Analysis Team, which is looking at the characteristic vulnerabilities that some of this malware uses. There is a Malware Analysis Team that actually looks at the code of the malware and exactly how it works, exactly what is being done and how malware might relate to malware. And there is the Insider Threat Team that is looking at some of the ways that people are tricked into accessing malware by phishing messages and so forth.

Suzanne: Okay, excellent. I do want to set a little bit of framing for why we are doing this podcast. One thing, ransomware cases are on the rise. It is in the news. The *New York Times* reported earlier this month, in October of 2020, that a woman actually died from treatment delays after a hospital in Germany was hit by a cyberattack, and they were forced to turn away emergency patients. So that is a pretty severe kind of result from a ransomware attack. There was also a coronavirus vaccine trial that was bogged down and delayed because researchers were locked out of their data, which is a common aspect of a ransomware attack.

You have talked about the spike in these kinds of cases in your recent blog post. Help our viewers understand what is going on and what is behind this increase in ransomware attacks?

Marisa: Ransomware is predominantly motivated by money. Cyber criminals want the money, and they have seen that ransomware is an effective way to do this. Organizations have been put into the terrible position that they need to pay a ransom in order to get back access to their hospital systems or the research that these people were doing for the COVID vaccine. Just know, I do not know if these specific instances actually paid the ransom. I am just using that as an example.

But in April of 2020, the RSA Conference was going on, and Supervisory Special Agent Joel DeCapua [of the FBI] presented research that he has been doing over the past six years. I think it was from 2013 to 2019. He basically tracked ransomware Bitcoin wallets, and he discovered that these different ransomware variants have collected over $140 million over those six years. When he was finishing that in 2019 Ryuk collected $61 million in ransom.

Suzanne: Those are amazing numbers to me. When you hear about, *Oh, somebody asked for $30,000 or $60,000 or whatever*. But this kind of number, $140 million over six years, is the kind of number that makes criminals pay attention to this as a vehicle for their criminal activity and for getting criminal funds. That, I think, is really important to note that this is not going to go away in the near term. It is too much money involved.

Marisa: Exactly, and like he even noted that it is likely even more money because he did not have access to all the ransom notes and all the Bitcoin wallets. So, it is likely even more.

Tim: Well, and ransomware is shifting. Back when it began, it was really more directed towards individuals. You know, *I have your home information. I have your checking account information. Pay up*. It has moved to prominently be focused on businesses and government organizations, government entities. Cities are getting hit, and when your police and EMS are out, that is very, very impactful. It motivates people to pay money, and so they can demand larger money. So, several cities in Georgia got hit in the last year.

Marisa: Going back to how you said that woman’s death was linked directly to the ransomware attack, it is honestly likely that there have been deaths that have not been able to be linked because of EMS services being down. You can’t really know, but like that probably has affected people’s health in ways that we could not directly connect to a ransomware attack.

Suzanne: What is the increase like in recent times? Because that is one of the things that prompted your blog post, I think.

Marisa: Yes, so ransoms themselves have been increasing. Ransom payments from Quarter 3 of 2019 were on average $42,000, and in Quarter 1 of 2020, that has jumped up $70,000 up to $112,000 is the average ransom payment now.

Suzanne: ...and the volume increased as well.

Marisa: Yes. The volume of attacks [has] increased by 25 percent in Quarter 4 of 2019. Then right when we go into COVID, in Quarter 1 of 2020, it just has increased by 25 percent. So, the ransomware attacks are not slowing down and are expected to increase. It has been, like we said earlier, it has proved to be a lucrative means to do this, so more and more criminals are doing this.

Tim: One of the differences is also the skill set required to run these attacks has shifted. It is not the ransomware authors that are running these attacks. Instead they have gone into the franchise business. You have franchisees, we call them affiliates, who are doing the ransomware attacks.

Suzanne: That is called ransomware-as-a-service, I believe.

Marisa: Exactly. That was what my first blog post was actually on. Ransomware-as-a-service is a new business model, like Tim mentioned, that allows the ransomware developers to lower their risk because they are not actually the ones doing the attacks anymore. They are either selling the ransomware or leasing it out to these different attackers. The attackers are growing because they no longer have to develop their own ransomware to form these attacks.

Suzanne: That is a scary blog post for me because I am thinking where we are kind of entering into this dystopian future where people that…It is bad enough when people with high technical capability turn their skills into this kind of criminality. But making this now available to people that do not have that level of technical skill, this is something I think businesses and organizations need to be paying a lot of attention to if they are not already.

Tim: We have seen this kind of evolution before. The initial distributed denial-of-service attacks were done by high-caliber, high-technical-knowledge people, and then they developed a toolset, and your average high school student could run it. It greatly decreased the level of technical sophistication required. In terms of spam, the initial spams were put together by people who really knew how the email system worked and how to tweak it to cause things to happen. Then they packaged it, and now it is being run very, very broadly for pharmacological spam, for fraudulent spam, things like that. It's happening again. That same sort of evolution is happening again with ransomware.

Marisa: It is already known that ransomware utilizes prefabricated exploit kits, so the exploit kits are basically how they can get into the network. Then they do not have to develop the ransomware, it is already made for them too, so they are just deploy it on the network and it is just bad news for organizations.

Suzanne: Yes, so I am going to take it back to like spam. When spam originally came out, I know I was one of the many people that was ready to throw my laptop through the window with all the spam stuff that I had to filter out. But IT organizations, people that are paying attention to this, like CERT, found strategies for preventing spam. Filtering is a big mechanism, and filtering at different boundary layers and things like thatm, so that now I get annoyed once in a while, but really in most end users' daily work, spam is not a defining element of their interaction with the email systems.

Are we going in that direction with the solutions to ransomware? I know that the FBI and others do not support paying ransom. What are we able to help organizations with so that they do not have to pay the ransom, so they do not have to be faced with that decision to either prevent a ransomware attack or respond once it has been executed?

Tim: Well, recognize that paying the ransom is usually a bad idea. One, you are rewarding the criminals, and that which you reward, you get more of. You are just adding to their cash flow and giving them more capability. Two, about 60 percent of the time that an organization pays the ransom, they either don't get back anything in terms of a decryption key, or the decryption key that they get back does not work. They pay the money, and they get nothing for it about 60 percent of the time. There is a variety of different studies that lead to that 60 percent figure. It is better to be thinking more in advance and prepping your own solution rather than depending upon the criminals, which kind of makes sense. I mean, what is the criminal's motivation [to help restore the victim].

In addition, even if the decryption works, the criminals make no guarantee that they won't turn around and hit you again. So the average organization that gets hit, gets hit about three times within the calendar year with ransomware attacks. It is really bad news to be paying off the ransom. Matter of fact, adding to the bad news, the Department of the Treasury is now proposing a set of sanctions against organizations that pay ransom, particularly within the financial industry. So, you not only could get hit by having to pay the ransom and putting all the effort into trying to secure your systems, you [may have to] pay a penalty to the government related to it. pay a penalty to the government related to it.

Marisa: To tie onto that, there are new behaviors with the ransomware from data exfiltration. So you can be hit for fines. If you have sensitive personal identifiable information or credit card numbers, you could be hit by fines for that too. Or now if you pay the ransom to get that data back, you could also be hit by a fine for that. So you need to take new strategies to protect your sensitive data.

Suzanne: Marisa, do you want to explain to those who may not know what data exfiltration is and how it relates to ransomware?

Marisa: Basically, before the ransomware attackers go into the network and encrypt all the data, they are going in, and they are actually downloading and stealing information off the databases and whatever they can get their hands on. In November of 2019, they actually did this to Allied Universal, and they told them like, *Hey, we stole some of your data, and we are going to publish it unless we get a ransom*. Allied Universal did not pay the ransom, and they ended up publishing 700 megabytes of the data online. It has only continued. Even more ransomware variants are adapting this to their strategies, and it is just becoming more and more common.

Tim: Maze actually has a name and chain website that they have set up just strictly for, *These are the organizations we have hit. This is their critical data. They did not pay the ransom, here you go.*

Suzanne: Wow, and here we are. One of the obvious strategies is, make sure you have backups of your data somewhere else so that if someone does get access to your data, you are not completely eliminated from accessing it. What are some of the other strategies that we recommend to organizations. If they are listening, hopefully if they have not already engaged in a ransomware strategy, they will be motivated to do so? So what are some things that they should be paying attention to?

Tim: Well, one of the things that you need to be aware of is the ransomware attackers know that organizations cut backups, and so they will target the backups first because the data is already gathered there for them to download. You need to first of all, secure your backups. Make sure that you have backed up good data, and as much as possible, use malware checkers or antivirus solutions or consistency checkers to make sure that what you are backing up is proper. Then encrypt the data yourself so that, even if they download it, they cannot publish it.

Suzanne: OK. Use their strategy against them. I like that.

Tim: There are several characteristic ways that attackers get into organizations to plant malware. The main one is the wide-open front door, which is email. The more you can do to spoil the phishing, if you will, make it so that people are less likely to click the links, the more robust your organization is going to be. That includes informing your people that, *Hey, we are likely to be targeted because, watch out for this, watch out for that, watch out for this*. Come up with very bulleted points that deal with protection of your critical information. Also, test your people after you have given them this training. Maybe not right away, maybe a week or so later. Run a phishing test against your organization and see who does click the link. Then cycle those people back into further feedback and further understanding of, *Hey, we explained to you, you should not click the link, and then we turned around, and you clicked the link*.

Marisa: Oh, another one of the main attack vectors is RDP [Remote Desktop Protocol]. A good strategy just in general is minimize your organization's attack surface. Like all of the stuff you have that is internet facing, trying to minimize that. If you do not need services, turn them off. If you are not using ports, lock them on your firewall. Just minimizing that, it just lessens the opportunity of attackers being able to get into your network.

Suzanne: So, reduce the opportunity on the front side, a couple of things you talked about there. Reduce opportunity on the back side by protecting your data, and I think I saw in one of your blog posts a statement about any data that you can think of that you would not want to be published on an external website, you probably want to encrypt. I think that is a nice rule of thumb for getting people more sensitized to, it is not just about losing access to the data, but some of the fines—an not just the fines, the loss of reputation associated with, *Hey, my data is not safe with you guys*—is something that organizations want to avoid. Are there any other big themes in terms of things that people should be watching out for either on prevention or recovery?

Tim: Well, those are basically your, we call them *table stakes* techniques. Which is, if you really want to be able to stand your own against malware, that is at least the base level for trying to deal with them. Then you have the more specific things that are geared around your critical assets. That, as Marisa commented, involves making sure that you are managing your attack surface, particularly around your very most critical assets. Marisa, do you want to highlight some of the points there because that was part of your blog post.

Marisa: Yes. So, besides the phishing and the backups, three other things that you should consider are reducing your attack surface, as I mentioned before: turning off services, blocking ports. Then you want to try doing a layered approach. You want to use firewalls to block those ports. You want to use host firewalls to block ports. You also want to use antivirus, as Tim mentioned. The last one is, if they actually do get on your network, then that is when you need to make sure you have those valid backups, and you can also have encrypted your sensitive information. Because like you said, if you are thinking, *Hmm, I would consider paying ransom for this data,* then you should just encrypt it, and then you will have peace of mind.

Tim: Beyond that, there are methods where, for example, you can apply deception on your network. Set up false servers that are much more exposed than the real ones that the attackers might want to go after. Use those for, one, knowledge that an attack is going on without losing data, and two, profile the attackers pretty definitely. *These are the vulnerabilities they are going for. These are the services they are exploiting. This is the phraseology in the email messages that* *they are sending.* Be able to gather that kind of data so that you can offer very specific warnings to your people, so that you can make sure that you are hardening your network against the specific methods being used.

There again, this is more investment, more effort. But if you really are very concerned about this threat and the large financial costs that could be associated, it may very well be worth it. And there have been some very, very high-profile cases where ransomware got involved. For example, a subsidiary of FedEx in Europe got infected through a supply-chain risk, and it took FedEx Europe down for several weeks. They actually had to end up passing business to competitors to try and deal with the problem. It was a mess and very costly.

Suzanne: The SEI, as most of our viewers already know, we are a federally funded research and development center. We are one of those places that gathers information about profiles, things like that. We call ourselves an honest broker. We try and anticipate and solve some of these problems, and convey them not only to the government, which is exactly what we are doing here. What are some of the things that we are doing? What are the projects and resources that we have to offer our audience in terms of either participating in our work, in our projects on this, or just resources that we have available that they can access?

Marisa: Recently both Tim and I have published separate [white papers] talking about ransomware. My report was on just like the current ransomware threats on the top ten ransomware variants that were active in the past two years. Tim, you can explain yours.

Tim: My report was looking at the NIST's CIF cybersecurity, pardon me, Cybersecurity Framework (CSF), cybersecurity framework. Then using the methods from the CSF specifically against ransomware. What is going to be done in terms of *Protec*t? What is going to be done in terms of *Prevent*? What is going to be done in terms of *Recognize, Respond* using the CSF methods?

Marisa: Yes, the NIST CSF methods and my technical report is a deep dive of ransomware and anything you want and different responses you could take. Then we also both wrote a blog post about this. I wrote one on ransomware-as-a-service threats. The second one, I believe Tim covered his acronym, which is, [SEE] **S**poil the Phishing…

Tim: Ensure good backups and Encrypt data.

Marisa: Then the final blog post, [now published here], is just talking about more defense strategies that you can do, which are reducing your attack surface. It is also like layering your security, and finally, encrypting sensitive data. The blog posts I think are pretty great. Because it also, it touches on stuff we at the SEI do and then also has other external sources. So you can determine how deep you want to go.

Tim: Yes, and these are not the first blog posts that have been done on ransomware. Several of the research groups here at the SEI have done posts on ransomware, but we are just continuing to try and keep abreast of this threat and provide timely information about the threat and how to respond to it.

Suzanne: Well, and this is one of those ones that we have seen evolution. As long as we are seeing continuing evolution of these kinds of malware strategies, we are going to keep tracking it and keep working on it, because we want to protect the data of the organizations that are serving, in lots of different capacities, our citizens and stakeholders all over the world.

What are you thinking about next? What is the research direction that you are following? Do you want to say anything about how you see ransomware evolving? What are some things that are on the cusp of emerging that you might want to bring forward to some of our viewers?

Marisa: I am considering writing a blog post just touching on basic incident response to ransomware. That has not been completely determined yet. That is something that I am considering pursuing, and just like tips that your organization can do to help make the process smoother.

Tim: I am interested in working with organizations that are leveraging the cloud and developing and probably authoring a blog post on what solutions specifically help to protect your cloud-based assets. There are some big advantages to the cloud in terms of cost of that. There are some costs associated with the cloud, particularly in the area of awareness, how you track what is going on against your cloud-based resources. It is often difficult and being able to provide some more specific guidance there is probably going to be worthwhile.

We are going to see the attackers continue to innovate. Let us face it, the money is there. They are harvesting so much of the dollar amount there that they are highly motivated to continue to innovate to make their attacks even more costly and effective. They are going to be starting to try and go in against even encrypted data, largely by going after endpoints. They are going to try and hit someplace that has authorized access to data that is otherwise encrypted. Moving more towards, not just storage-based solutions, but endpoint-based solutions is probably something they are going to do and something that we need to pay attention to.

A lot of the network defenses that we have in place have largely been order- or server-based defenses. Now we are going to have to start suddenly paying more attention to workstation-based defenses or other sorts of attacks at that point. In addition, I would expect that attackers are going to look for places where data already exists and is congregated. So common storing solutions using network storage options, such as OneDrive or BOX or Google Cloud or things like that.

They are going to look at what solutions work for organizations that are using these types of systems and how they can easily extract the data out surreptitiously.

Finally, you can expect them to continue to innovate in terms of how they get people to click their links. They are going to continue to try and move things forward so that, when you are getting a message that gives them access, there is nothing in the message that triggers your alarm and says, *Oh, wait, this one is bad. In fact, it looks very, very good. It looks normal. I am getting email from Marisa. Marisa says, Hey, check out this file.* Okay, I would probably click the link. So being able to get more detailed understanding of organizations and how to couch more direct attacks to make them more effective, that is probably a direction that the attackers are going to go, which means we as defenders have to be more alert as to, *What is the evidence that this really does not come from Marisa, it comes from J. Evil Person that is out there?* There is a lot of interesting work in this area. It just remains to be seen how things evolve.

Suzanne: Which means that we are going to continue to pay attention to it, and you guys are going to keep writing blog posts and reports to help people understand what they can do. As these threats evolve, we will be there to help people understand how to mitigate those. That is what we do. I want to thank you both for doing this interview. Remote is always harder, but we are getting the hang of it. But thank you for talking about this work. I think it is very important if you are a viewer who is just coming into the ransomware arena, pay attention because this is not going away.

To all of our listeners, we mentioned some technical reports and other blogs. All of those links will be in our transcript. We do that for all the resources that we mention in a podcast. Thank you for joining us today. As always, if you have questions, please do not hesitate to access us at info@sei.cmu.edu. We hope that you will get this podcast wherever you get your podcasts. Thank you for viewing.

Thanks for joining us. This episode is available where you download podcasts, including SoundCloud, Stitcher, TuneIn Radio, Google Podcasts, and Apple Podcasts. It is also available on the SEI website at sei.cmu.edu/podcasts and the SEI's YouTube channel. This copyrighted work is made available through the Software Engineering Institute, a federally funded research and development center sponsored by the U.S. Department of Defense. For more information about the SEI and this work, please visit www.sei.cmu.edu. As always, if you have any questions, please do not hesitate to email us at info@sei.cmu.edu. Thank you.