EPISODE 334

[INTRODUCTION]

[0:00:00.6] JM: Ransomware uses software to extort people. A piece of ransomware might arrive in your inbox looking like a PDF, or a link to a website with a redirect. Ransomware is often distributed using social engineering. The email address might resemble someone that you know, or a transactional email from a company like Uber, or Amazon.

Tim Gallo and Allan Liska are authors of the O'Reilly book; *Ransomware: Defending Against Digital Extortion.* They join me to describe the five stages of ransomware; deployment, installation, command and control, destruction, and extortion. Tim and Allan describe conditions under which it might make sense to pay the extortion and some frightening recent cases of ransomware impacting the real world.

We'd love to get your feedback on Software Engineering Daily and how it impacts the real world. Please fill out the listeners' survey available on softwareengineeringdaily.com/survey. Also, Software Engineering Daily is having our third meet up, which is Wednesday, May 3rd at Galvanize in San Francisco. The theme of this meet up is going to be fraud and risk in software. We're going to have some great food, engaging speakers, and a friendly, intellectual atmosphere. To find out more, go to softwareengineeringdaily.com/meet up, and hope to see you there.

[SPONSOR MESSAGE]

[0:01:35.6] JM: Deep learning is at the forefront of evolving computing and promises to dramatically improve how our world works. In order to get us to that bright future, we need new kinds of hardware and new interfaces between this AI hardware and the higher level software. That's why Intel acquired Nervana Systems, a platform for deep learning.

Intel Nervana is hiring engineers to help develop this full stack for AI, from chip design to software frameworks. Go to softwareengineeringdaily.com/intel to apply for a job at Intel Nervana. If you don't know much about Intel Nervana, you can check out the interviews that I've

conducted with engineers from Intel Nervana, and those are available at softwareengineering.com/intel as well.

Come build the future of AI and deep learning at Intel Nervana. Go to softwareengineering.com/intel and apply to work at Intel Nervana. Thanks to Intel Nervana for being a sponsor of Software Engineering Daily, and I really enjoyed the interviews I have done with the Intel Nervana stuff. I think you'll enjoy them too.

[INTERVIEW]

[0:02:58.0] JM: Tim Gallo and Allan Liska are the authors of *Ransomware: Defending Against Digital Extortion.* Tim and Allan, welcome to Software Engineering Daily.

[0:03:06.9] AL: Thank you very much. We appreciate you having us on.

[0:03:09.9] TG: Yeah, thanks Jeff.

[0:03:10.9] JM: Ransomware uses software to extort people. Stories about ransomware are sad and frightening, but they can also be somewhat entertaining. They can be interesting and instructive. You are both heavily engaged in this space, and I want to start with a story from each of you about ransomware. It can either be a brief news story that illustrates a type of ransomware, or maybe a person who told you an anecdote, or something that you dealt with personally. Tim, why don't you go first?

[0:03:43.5] TG: Sure. One that comes to mind actually is an interesting situation. It was kind of all over the news when the ransonware infections happened at the Healthcare Center based in the Baltimore area. A friend of my partner's on her way to go get her chemotherapy at that health center and she got there, everything was getting setup, and she was told basically to go home. That they weren't able to give her her chemo today, and that they weren't able to get into the systems or schedule anything, they would have to call her at some point in the future to be able to get her chemo.

Now, this is one of those things where missing a day of chemotherapy when you have advanced cancer is not only potentially dangerous, but it put her life at risk. It was a few days before she ended getting a call to get rescheduled when they had finally remediated that the ransonware, and that's a kind of thing that just kind of breaks your heart when you see how something like this can happen and the types of effects that that can have on — The real human effects that ransonware is going to have on people.

[0:04:52.9] JM: Yeah. We'll look back to that example, because that's one of the most alarming examples that happened recently. I think we'll come back to both of these anecdotes, whichever they are as cases and point. Allan, what's your example?

[0:05:05.8] AL: Oddly enough, mine also has to do with healthcare. I'm in the Washington, D.C. area and got a call from a friend of mine panicking because of the MedStar attack. Very similar, although not quite as severe, basically freaking out, because she couldn't go see the doctor that day simply because they were shut down until they could figure out what to do. It was not as severe as Tim's example, but yet another example of somebody just denied healthcare because of ransonware and having no idea what to do, or what it meant, and what the implications were not just for her treatment, but for her medical records and so on and what that was going to mean to her.

[0:05:52.2] JM: What's MedStar?

[0:05:53.6] AL: MedStar, it's a hospital group. I don't know how big it is around the county, but in the Washington, D.C area, they own several of the hospitals. In somewhere of last year, they were hit with a ransonware attack that shut them down for several hours.

[0:06:11.5] JM: We'll go into a dissection of ransonware in a second. There are several families of ransonware. Before we get into the anatomy of a ransonware attack, give an overview of some of the types of families.

[0:06:23.2] AL: Yeah. Broadly speaking, there are two different types of ransonware. Locker ransonware, which denies you access to a system. You see that most commonly on cellphones.

You get a popup window that says, “Your phone has been locked by the FBI,” or whatever, “and until you enter in $50 worth of iTunes gift cards, you can’t have access to your phone.”

Then, there’s also the crypto ransonware which is the one that where most people are more worried about and is more common and generally affects PCs, and that is ransonware that infects your system that when it’s downloaded, encrypts files and doesn’t allow you to have your files back until you enter in a key, and that usually — Then you pay using generally Bitcoin to get that key, you enter in the key, and hopefully get your files back.

The biggest example of that today is server which is the sort of the king of that, but you see Spora, you see Locky not as much, but that recently was a big one, and a few others like that.

[0:07:35.2] JM: Okay. Let’s break down the anatomy of a ransomware attack into the five stages that you two described in your book. There is deployment, installation, command and control, destruction, and extortion, finally. Let’s start with deployment.

Tim, what happens in the deployment stage of a ransonware attack?

[0:07:57.7] TG: Extensively, when dealing with deploying ransonware, the criminal actors are going to find one of a few different methods to try to get the initial infection on to your system. The two primary methods that they use are via email or via some form of WebKit attack, and we see there’s a pretty broad collection of attacks between the two.

From an email perspective, it can be anything as simple as having these attachments in an email where you open the attachment and initiates the downloader, that will then download the primary infection and begin the installation phase. From a WebKit perspective, it’s a little bit different in so much as there may be malicious code hidden inside legitimate or illegitimate websites, or links back to illegitimate websites that are hosting these exploit kits.

When they see the browser footprint that you’re presenting, they can validate — They can exploit specific vulnerabilities inside the browser that you’re leveraging and use that to sort of choose which ammunition that they’re going to use to drop a piece of ransonware at the end of the day actually to drop the code that will eventually install the ransonware.

What's interesting is, in many of these cases, they also use your location information to identify where you're at so they can leverage appropriate language. If you're Germany, they want to make sure that they're posting everything up in German. If you're in the United States, they want it to be in English. If you're in Russia or the Ukraine, they don't give you the ransonware at all.

[0:09:26.7] JM: Tim, what are some of the more creative ways that you've seen ransonware delivered to someone's computer?

[0:09:32.5] TG: One of the most interesting and it's ridiculous that it works, but it does, is just the simple email that you see, your UPS package is being delivered, or your UPS package has been delivered. That's something that people will click on without even thinking. If that's a link back to a ransonware drop site, it's almost an immediate methodology for getting the information and the malicious code down to somebody's system.

That in and of itself is so simple and yet so sort of sublime and that it just continuously works, because people want to do that. There are many nefarious ways and many more intriguing ways, but sometimes just simple is all you need.

[0:10:18.1] JM: You both write about some preventative measures that can help ward off ransonware deployment. These are measures such as Edge sandboxing and BareMetal detonation. Allan, why don't you describe some of these?

[0:10:33.5] AL: Sure. There are two different approaches to how you protect yourself against ransonware. There are the Edge defenses that you described and there are a lot of great ways of doing that. It's not enough just to have a mail system, like a mail filtering system. You almost need a mail sandboxing system, something that's going to take those attachments and actually detonate them and see what they do, especially if they're compressed if they're compressed with a password. Those type of things you really need to take a look at, because that's some of the methodology.

That's one way that it can be done when you're talking about intercepting email, same thing with web-based attacks. Having a proxy that is constantly checking for new bad links and verifying those links, sandboxing a technology that sits between the user and the internet that is looking at anything that's trying to be downloaded and examining it first, putting it back together.

Sometimes there can be challenges with that, especially as we move to fileless ransomware where it's simply a script, or it's base 64 encoded and doesn't become an executable until it hits the desktop. In that point, proxies and sandboxing can be more of a challenge, or can be less effective.

I also recommend using a next generation endpoint solution. Using like a SentinelOne or a Carbon Black or something like that that's looking at the behavior so that even if this file is malware, it doesn't become an executable until it hits the desktop or it never becomes an executable. The fact that it's doing certain things can get flagged and alerted on. Things like using Vssadmin to delete shadow copies. There's no legitimate reason for doing that, or starting — It's a little late then, but starting a mass encryption of files. That's not good. Go ahead and cut that off, and that way you only lose a couple of the files to the ransonware.

The other half of that, and I'm sure we'll talk more about this soon, is educating the users. Keeping them aware of what's going on. Having them maintain that situational awareness and security. I think we make the mistake of thinking our users are too dumb to do anything and kind of blaming the users when they fall victim to these. I think it's on us, in security, to do a better job of communicating with users what to look for and what to be on the watch for. That's the other half of this type of protection.

[SPONSOR MESSAGE]

[0:13:37.6] JM: Software engineers know that saving time means saving money. Save time on your accounting solution. Use FreshBooks Cloud Accounting Software. FreshBooks makes easy accounting software with a friendly UI that transforms how entrepreneurs and small business owners deal with a day-to-day paperwork. Get ready for the simplest way to be more productive and organized. Most importantly, get paid quickly.

FreshBooks is not only easy to use, it's also packed full of powerful features. From the visually appealing dashboard, you can see outstanding revenue, spending, reports, a notification center, and action items at a glance. Create and send invoices in less than 30 seconds. Set up online payments with just a couple of clicks. Your clients can pay by credit card straight from their invoice. If you send an invoice, you can see when the client has received and opened that invoice.

FreshBooks is also known for award-winning customer service and a real live person usually answers the phone in three rings or less. FreshBooks is offering a 30-day unrestricted free trial to Software Engineering Daily listeners. To claim it, just go to freshbooks.com/sed and enter Software Engineering Daily in the How Did You Hear About Us section. Again, that's freshbooks.com/sed.

Thanks to FreshBooks for being a sponsor of Software Engineering Daily.

[INTERVIEW CONTINUED]

[0:15:19.0] JM: After deployment, the next phase of ransonware is the installation event. Tim, what typically happens during an installation event?

[0:15:31.2] TG: Each family kind of have their own unique methodology once they've gotten on to the system itself. Extensively, what we're looking at is they leverage some form of dropper and downloader install tool. Once they've gotten into the system either through a PowerShell script, because they're a fileless piece of ransonware or they've gotten into the system through some of the more traditional means through an infected file, or through a link. That initial case, in many cases, that's going to make its connections out to its CQ channels and ensure that it's got the appropriate code to begin the process of installation. That's getting all of its DLL hooks in place, ensuring it has appropriate system admin rights to begin the process of encryption or browser locking depending upon — Again, we're primarily talking crypto ransonware in this case, but to begin the processes of identification of files and encryption.

It establishes itself extensively like any piece of malware on a system. What it's going to do is get all the appropriate permissions to perform the action it needs to do as well as ensure the

communication paths are clear. At that point, we often see — Then it will begin the process of identifying the files that it wants to encrypt, or the resources that it would like to lock. In the case of file encryption, primarily, they're looking for things; Words documents, looking for JPEG, bitmap files, looking for things that are of value, Office documents, stuff like that.

Depending upon the end user, the value could primarily be in your Word, Power Point docs, or if it's consumer end user, or your home system, the value primarily there is in things like your pictures. It does blanket searches across the environment for those files, begin to identify them and then starts the encryption process in the case of crypto lockers, or crypto ransonware in general. That's what it's primarily doing, encrypting them with the embedded keys that are associated with the malware itself.

[0:17:28.8] JM: After the installation phase, there is the command and control step. In this step, the ransonware takes control of the computer. It contacts the command servers, looking for instructions. Allan, explains what happens in the command and control transaction.

[0:17:50.7] AL: Sure. Note; not all ransonware uses the command and control phase. Some of the ransonware — Some ransonware families have opted out of that simply because they want to keep everything self-contained out of fear of having the process disrupted.

Generally speaking, what happens is once the ransonware is installed and everything is encrypted or even during the encryption process, the ransonware may have to reach out to the command and control sever to get the key, to get the private key in order to do the encryption. Once it's done, it sends a note over to the command and control host saying, "Hey, we've infected this system," and it gives the details about the system that's infected.

There are a couple of reasons for that. One, bluntly, metrics, so that the ransonware developers can keep track of the systems that are being infected, how it got infected, what the history of the installation work was like, what worked, what didn't work, and so on. Also, a big part of ransonware, and frankly, a big part of the success of ransonware is ransonware is a service where a novice or a neophyte who wants to get into the ransonware business but doesn't want to develop their own ransonware will use somebody else's ransonware and the check-in allows

them to verify that, “Yes, I’ve had this done.” They can go check the portal and see how many victims have successfully had the ransonware installed.

At that point, the check-in is simply, “Hey, we’re in. Here’s the information about the system and the files have been encrypted,” or “We weren’t able to encrypt everything. I was disrupted,” or whatever. Now, there’s the other part of that where ransonware doesn’t always operate alone. There are some ransonware families that will throw down ransonware but then also throw down an info stealer, or a keyboard logger, or whatever.

Those secondary pieces of malware will be also calling back to the mother ship to report in with any keystrokes logged, with any information that was able to be stolen, et cetera. There are really two reasons for it to check-in.

[0:20:17.0] JM: You mentioned some of the services, some of the ransonwares do not want to do a command and control, is that because in order to reach out to an external server, you might accidentally expose who the bad actor is? Because if you reach out to an external server, presumably you’re reaching out to, “Hey, calling home,” and then if there’ s a trace from that to the bad actor, that could be incriminating, or is it for a different reason?

[0:20:49.2] TG: It’s got less to do with incrimination, because in most cases there are so many layers of obfuscation between the criminal actor and the supporting command and control infrastructure. They got more to do with disruption. If I’m doing a good job of monitoring outbound web traffic and I’m running SSL decryption across my environment and identifying outbound communications. To see those types of comps to know in CQ channels or suspicious URLs, things that look like DTAs, that allows me to, as a network defender, to interrupt the communication and potentially quarantine and/or enforce a wipe and rollback on those end user devices potentially.

It’s an attempt to avoid the disruption, less about the incrimination. Very rarely do we actually see these guys get caught because of these communication paths. That is something that eventually through large scale analytics, you can do, or if somebody is poorly coded their system or hasn’t put in the appropriate layers of obfuscation, they can. In most cases, there’s enough layers of that that it’s very difficult to find the actual bad guy.

[0:21:58.7] JM: Allan, the final two phases are destruction and extortion. Can you describe what happens in these two stages?

[0:22:06.1] AL: Sure. Destruction can mean one of two things. Generally, destruction is getting rid of any system, any unnecessary programs. Whether that's the loader, whether that's the initial executable, anything that's not needed. You don't want to leave any evidence behind for forensic analysis. There's already enough forensic capability, so unlike other types of malware which tries to be stealthy, most ransonware developers are proud of their ransonware and they'll include the name, "You've been infected by Cerber, or by Locky, or CryptoWall, or whatever."

That will be in the ransom node. It will be based on what the extension that's used. The identifying information is there, but they don't necessarily want to leave behind how they got on the system. There'll be that kind of clean up. Then, there's some ransonware that isn't really ransonware, it's just there to destroy files, and so it will popup a ransom note, but it will actually destroy your files in the process. There are no files to recover.

For ransonware, that's not like that. The ransonware that is — Then the recovery part is the person pays the ransom, the victim pays the ransom with however many Bitcoin it is. They're given a key. They enter the key and that allows them to decrypt the files, hopefully.

[0:23:42.3] JM: Yeah. Let's get into the discussion of the ransom. In your book, you talk about the factors that a victim should consider when deciding whether to pay the ransom. What are those factors that they should take into account?

[0:24:00.5] TG: Obviously, the first thing you've got to take into account is similar to the stories that we had talked about today is how fast can you get your business up and running, and are lives at stake? That's, I think, a key component there. In many cases, like the two that we discussed, I can't remember off the of my head now and you'll have to correct me. I think I know in the one they did not pay the ransom, they just recovered everything from backup. I don't know about the MedStar off the of my head. Allan, you probably have more details on that one.

Extensively, that's one of the first things you got to consider is what are the impacts to business

operations? If you've taken the appropriate steps and built incidence response playbooks that include things like, "How do I respond to ransonware?" "Do I have effective backups?" "Am I doing sort of continuous backup and monitoring of the devices?" "What's the size and scope of the infection?" "Do I have map to drives all over my environment, and because this system was infected, it's actually infected a number of my servers as well because they've had map access to these drives?" Those are all factors to take into account from an information architecture perspective.

When you're looking at it in a smaller home environment, it just comes down to, "Do you have backups of all your pictures of everything that you want to keep?" "What have you done to protect yourself preventatively," by doing those preventative steps, it makes it so you shouldn't have to pay the ransom and instead can just restore those lost backup.

One of the things that happens a lot though is people don't test their backups. Not only do you have recent backups, but have you validated them. Are they actually working? If you're using tape, are the tapes available, or are they sitting there somewhere else? If you're a disc, have those discs been compromised? Do you know if they have or haven't? Has your detection of the ransonware map to when the last backup was? Did you actually backup the locked files unintentionally? These are the things that you got to take into account when you assess. Is it appropriate for me to say, "Forget about it, I'm just going to full from the backup," or "This is serious. I need to get up and running ASAP." If I had my way, we would never have to pay the ransom simply because you're contributing to their research and development. By funding these criminals, you're just extensively funding them to continue to make their product, their ransonware more effective and any other criminal activity they may be engaged in.

[0:26:26.2] JM: Who falls victim to ransonware? Is it always big companies and hospitals, or is it also individuals?

[0:26:36.6] AL: It's interesting because ransonware is somewhat indiscriminate, especially ransonware delivered via email. At the height of its popularity, Locky, the team behind Locky was sending out 10 million emails a month. They weren't just hitting corporate networks, they were hitting individual networks and so on.

One of the really fascinating things we found out in doing the research for our book was that the home email providers, so that Gmail, outlook.com, and even to some extent, yahoo.com, actually do a really good job of filtering out ransonware emails. The home user rarely sees them. At any given day, if I need a ransonware sample, I can go into my Gmail spam folder and I'll have a half of dozen of them that I can pullout and use as a sample, but I never actually see them in my inbox.

While home users are getting hit just as often as commercial users, they aren't seeing the ransonware as often, and that's because many businesses don't have the type of protections that they need in place. They aren't running a mail filtering software, and they're certainly not running email sandboxing or anything like that. Those protections aren't there because — I don't want to say definitely because, but it seems to me that most companies are focused on protecting the network at the edge, not thinking about email as actually part of the edge. Strong firewalls, strong IDSs, strong proxies, but not necessarily strong email protections.

[0:28:36.2] JM: Who are the perpetrators who are making ransonware?

[0:28:41.8] TG: The manufacturer, the code writers themselves, typically fall down to — It's actually a fairly small group I would say. There's a few different families. I think we're tracking, I guess, it's may be 12, 13 total families that I've got that I'm monitoring myself, but it's not a lot. These are all criminal organizations that are in this for financial gain. It's not something that's handled through nation state actors.

However, based upon a lot of the geo-fencing that we see in ransonware infections in particular, it would lend itself to believe that most of the folks that at least are in the samples that I've seen are in Eastern Europe, primarily, Russia, Ukraine, those area simply because there's a lot of geo-fencing that prevents installation and deployment of the ransonware inside the end user environment in those area particularly to avoid prosecution.

[0:29:39.3] JM: You're saying that because the ransonware itself has been written in a way that prevents it from being installed in Russia or the Ukraine, that is indicative that probably the people who are writing it live in those places.

[0:29:57.3] TG: Yeah, and that's a twofold thing. One, you wouldn't want to infect your mom's computer or your neighbor's computer. Two, and I think that the more important reason, is by not performing the criminal activity inside your legal boundary, if you will, whether that's a nation or a province or whatever it happens to be. You're limiting the risk that you have from criminal prosecution perspective simply because it's no longer local resources that are attempting to catch and arrest you and prosecute you.

Instead, it's international resources that have to rely on cooperation with local resources. If you're making that tens of millions of dollars necessary to do this on the backend of something like this, it's possible that — Again, this is all hypothetical and alleged in these cases, but that you could protect yourself very effectively with good lawyers and/or good criminal protection.

[0:30:51.0] AL: In other words, nobody wants to get to a Russian jail, even people in Russia?

[0:30:55.0] TG: Yeah. Much better put, Allan. Thanks.

[0:31:01.2] JM: Are the people who are making ransonware the same people who are deploying it?

[0:31:07.0] AL: Really good question. There does seem to be some overlap with some of the teams. The Locky ransonware was exclusively using Dridex infrastructure, so that kind of ties in — Yes, those two are connected, but then you see things like Spora or Cerber that bounce around from different types of exploit kits and different types of delivery methods, which tells me that they are focusing strictly on developing the ransomware and making the best ransomware possible; and then writing out these exploit kits or renting out the botnets that deliver this spam and allowing those people to be really good at what they do.

We're going to make the best ransom ware possible. You make the best exploit kit possible or you make the best span delivery system possible. Really, that specialization, they'll focus on what they do and count on the fact that there's already an infrastructure there for them to piggy back on, and they can take advantage of it. Of course, they're making enough money that they can afford to rent that out and pay it.

[0:32:25.6] JM: Have you guys met any or the perpetrators in this space; either people who are writing it or distributing it?

[0:32:31.5] AL: I have not met in person. However, a lot of the ransom ware developers have chat support rooms. I've had a couple of conversations with them. They are surprisingly engaging and very willing to share information to a certain point about what they're doing and how they go about it and so on. It's really an interesting conversation to have and so on. Nobody's invited me into their home yet, and that's probably a good thing. I'm not sure that I want to go to Estonia, or the Ukraine.

[0:33:10.9] JM: What drives these people?

[0:33:12.9] TG: Money. Thinking about this from the perspective of economics, looking at the traditional methods for creating value out of hacking when you're criminal. Primarily, your target in the past where things like, "Okay, I would go try to drop keyloggers so I could get passwords and usernames for banking websites, so banker Trojans. I would attempt to install myself in point-of-sale devices to be able to grab untokenize or to be able to grab card stripe data, so I can replay transactions and steal that. To go after big fish and try to get large volumes of credit cards, so I can use them and resell them," or something along those lines.

Those all require multi-tiered infrastructures to be able to sell the information that you've stolen or to be able to somehow monetize it. As a criminal, why would I want to give 40% of my take to somebody who all they're doing is reselling what I've managed to steal? If I can find a way to go directly — Again, using economic terms, and I can find a way to go directly to my consumer, in this case, the person for whom I am installing the ransomware, and get money directly. Why wouldn't I do that?

Then, I can find alternative methods to monetize and create value out of my work product. I've developed these ransomware, it manages to get past all the current network email and endpoint detection capabilities. I've got this, I've made my couple of million off of it. Now, I want to make additional money. Let me set up a service where people can sell me, they can bring me giant lists of email addresses, or we can partner with spam bots for delivery of these emails and get these directly out the consumers. Now, I've created a business network extensively where I can

share in the proceeds and continue to make revenue off of a product that may be a generation or too old.

[SPONSOR MESSAGE]

[0:35:17.6] JM: Deep learning is at the forefront of evolving computing and promises to dramatically improve how our world works. In order to get us to that bright future, we need new kinds of hardware and new interfaces between this AI hardware and the higher level software. That's why Intel acquired Nervana Systems, a platform for deep learning.

Intel Nervana is hiring engineers to help develop this full stack for AI, from chip design to software frameworks. Go to softwareengineeringdaily.com/intel to apply for a job at Intel Nervana. If you don't know much about Intel Nervana, you can check out the interviews that I've conducted with engineers from Intel Nervana, and those are available at softwareengineering.com/intel as well.

Come build the future of AI and deep learning at Intel Nervana. Go to softwareengineering.com/intel and apply to work at Intel Nervana. Thanks to Intel Nervana for being a sponsor of Software Engineering Daily, and I really enjoyed the interviews I have done with the Intel Nervana stuff. I think you'll enjoy them too.

[INTERVIEW CONTINUED]

[0:36:42.0] JM: Do you meet white hats in this space who used to be black hats, or used to distribute ransonware or build ransonware and they've since come white hats?

[0:36:52.5] AL: No, I didn't see anybody in this space, but that doesn't mean they don't exist. That is not a group of people that I've met. Part of it is ransomware is relatively new, so even though there have been a number of high profile arrests and busts and so on, I personally haven't met anybody who has worked with ransomware and then switched over to the white hat, or become a white hat. I don't know. Tim, have you?

[0:37:21.5] TG: No, not in this case. Part of the reason, I think, is simply because we're still on the highly financially viable side of it. They're still making good money, and the few folks that have been busted and are in jail right now, I haven't heard of any of them flipping, going full white hat yet.

[0:37:39.1] JM: That's right. Remorse only comes when it's convenient.

[0:37:41.9] TG: That's true.

[0:37:43.4] AL: Absolutely.

[0:37:45.6] JM: Do you know of any of these ransomware gets delivered via adware? If you go to website where the advertisement inventory is not safe, and you click on the wrong ad and you get ransomware?

[0:37:45.6] AL: Yes, absolutely. While email makes up the primary delivery mechanism, exploit kits and especially exploit kits delivered by a malvertising, that's the second common way of delivery. There are a lot of different ransomware families that have gotten their start that way, because it's somewhat easier. That's where we also have seen a lot of the development in the file this ransomware. Ransomware delivered entirely is a JavaScript file, or something like that, where that has been delivered traditionally through a malvertising.

[0:38:43.2] JM: Let's talk about some of the popular ransomware today. Last year, there was Locky released. What does Locky do?

[0:38:53.7] AL: Locky is actually faded out as far as we can tell. There's been a huge drop off since the end of December in Locky distribution to the point where it's just a trickle. Locky is very traditional in terms of ransomware. It's an executable that's generally pulled down from an office attachment, so you have a Microsoft Word attachment. You open it up. It says, "Oh, you need to enable macros." The Macro will either call a PowerShell script which then pulls down the Locky executable, or depending on which version of Locky, et cetera, that you're talking about. The macro may actually pull the ransomware executable down directly. You hit that

ransomware, it executes, it runs, pay the ransom or don't pay the ransom, but your system's encrypted.

Locky was by far the most popular ransom ware delivered last year. By some estimates, the people behind Locky pulled in more than $300 million last year.

[0:40:06.5] JM: Wow!

[0:40:06.7] AL: Just a little bit less than Tim makes in a year.

[0:40:10.6] JM: Okay. You guys talked about these health care systems earlier that got attacked. What was the ransomware that attacked those hospitals?

[0:40:19.5] TG: I'll be quite blunt. I don't know the specifics behind which piece of ransomware it was that hit that friend's hospital. After she got that call, they gave her probably a little more information than they should. She did a little baseline social engineering to find out exactly what was going on, because obviously, she was very distraught, and they just had told her that it was ransomware specifically.

As far as the MedStar attack goes, I cannot remember exactly which one it was. You remember, Allen?

[0:40:49.0] AL: I'm not sure that they released the name of it. I do know that it was delivered as an attachment. I think with most of the medical ransomware that we've seen that's been primarily delivered as an attachment, generally, what looks like an invoice click open, et cetera. Most of the healthcare systems that we've seen that get reported as an infection don't list the specific ransomware that was involved in the attack.

[0:41:21.8] JM: If you're a victim and you decided to pay, how are you typically making that transaction?

[0:41:29.3] TG: Primarily, you're somehow acquiring Bitcoin. If you don't have a Bitcoin wallet, you're leveraging Bitcoin to pay these guys off. Typically, there is a URL or a string where you're supposed to enter the Bitcoin information and pay them in that way. That's the easiest way. Now, some the ransomware associated with mobile devices, they really tend to use a lot of different things. Some of the older variants, say, we're talking a few years ago, didn't use Bitcoin. They use prepaid Visa cards. They give you specific instructions. Then, some of the mobile variants, it's get iTunes cards. Those, however, really aren't quite as common, I think, today. It's primarily bit coin as the methodology for payment.

[0:42:11.6] JM: We talked about the different platforms that you can target with ransomware. What are we talking about? Are we talking about only Windows machines, or is it also Mac and mobile devices?

[0:42:25.0] AL: We have seen limited success in targeting Macs. KeyRanger was probably the most successful Mac ransom ware, but it wasn't done through exploitation. Instead, with KeyRanger, it was a trojanized file, so it was a BitTorrent downloader that contained ransomware. If you downloaded this particular BitTorrent downloader and execute it, it actually was ransomware, so you had to forcibly execute.

We have seen some science fair projects that targeted Linux systems that theoretically showed how you could execute ransomware on a Linux system. It is possible. We haven't seen anything like that in the wild that targets human interaction of enabling ransomware. What we have seen is the MongoDB ransomware where there is a [inaudible 0:43:26.5] in MongoDB and somebody wrote a bot that would encrypt it and then demand ransom. That's a little bit different than what we're talking about here.

It's still the same concept though. If you want your database back, you need to pay us in Bitcoin. Then, we haven't seen any crypto ransomware on mobile devices. Theoretically, it's possible on android to do that, but really, we see pretty much all locker stuff. We don't see any encryption, because most people back up their mobile devices to the cloud, at least at some level, and so it's very easy just to wipe and replace, wipe and restore your mobile devices. Go ahead. I'm sorry, Tim.

[0:44:11.3] TG: I was going to say, yeah, on the mobile devices in general because there's a lot of cloud interaction directly on those devices because the snow paw print. Until somebody has developed a ransomware that not only is encrypting the files on device but also in the cloud, it'll primarily be focused on the locker-style ransomware.

[0:44:29.9] JM: We saw with Mirai botnet what can happen when we have unsecured devices high jacked. For those who don't know, Mirai botnet was this botnet where you had a camera distributor or a camera manufacturer that puts a full Linux distribution in every camera and they use the same user name and password on all of the cameras that they produced, and then the Mirai botnet was this botn net that just went out and scanned the internet for cameras that fall under that description and tried logging with the default username and password they were able to.

The Mirai bot net was harnessed to lay DDoS against Amazon, which knocked out Netflix. Oh, gosh — I guess, it was Dyn or I guess DDoS Dyn. Anyway, the DDoS was horrible. What I think is you take over a camera, and you could just take pictures of somebody, and then use the pictures as ransom. Does it seem to you guys like we are in the earliest of the early days of ransomware?

[0:45:45.8] TG: One thing that I think is the idea that we've got where we're talking about ransomware specifically going after denying somebody access to a system or their files as the primary thought process for ransomware. That's one thing that we definitely look at. We're thinking about it today. That's how we react to it.

The next step, and we're seeing this happen a lot, where just like the Dyn attack using Mirai, is that I'm not just denying you access to your system or files by dropping something on your endpoint that is causing your endpoint to be useless, but I'm denying you access to your system or your network or your files by pointing a different weapon at you.

In the case of Mirai, by pointing that botnet at you and saying, "I will make your network unusable unless you pay." Extensively, extortion is extortion, and so that is also requesting a ransom. There are those that definitely disagree with me on this, but in my mind, that's an extension and that next step is how else can I take over things or do things to get money directly

from somebody as opposed to trying to steal something and then sell it. How can I just get money directly from people?

I think taking photos of humans using these cameras and then attempting to ransom them, attempting to extort them in some way is a little more complicated, because you've got to have additional levels of background on the person themselves to know, "Hey, it is something that they wouldn't want to get out that they were pictured going into a hotel at two in the morning or something like that?" The amount of additional work associated with that unless you're targeting somebody very specifically, probably isn't as high volumetrically speaking from a monetary perspective.

[0:47:34.4] AL: I think Tim has won an excellent point as far as ransomware in moving from just I'm going to lock out your PC to what can I do to embarrass your business. We saw that with the San Francisco community system. Now, they didn't pay, but that was the whole point behind this, "I'm in your system. I can show everybody in the world that you've been compromised unless you pay me, or I am showing everybody that you've been compromised, I've embarrassed you. Now, you should pay me because otherwise, I could make it worse." I'm a bit of a contrary when it comes to ransomware or an IOT only because most IOT systems are headless.

Now, that's changing where you talk about — Everybody likes to joke about the connected refrigerator and toasters, et cetera. If they have little screens on them, maybe that's different. If you infect my router — So if I've left my router unsecured, you infect it and you install ransomware; I will never know about it. My Internet may stop working, so I'm going to call my ISP and say, "Hey, fix my Internet." They're going to be, "Hey, we don't know what's going on. We're going to send a new router." I'm going to get a new router and plug it in. I'm never going to know that that router was infected.

Some technician back at Verizon might know that eventually, but I personally will never know about it. Even then, as disposed was a lot of these home routers are, Verizon probably takes it and drops it to be recycled somewhere. They may never find out about it.

[0:49:12.9] JM: I know we're up against time. You guys have been in this industry for a long time. What do you do on a day-to-day basis? Are you writing software or are you consulting with companies? Let's close off — Just describe what your work is.

[0:49:28.7] Allen, I think yours is so much more interesting. You should go first.

[0:49:33.0] AL: I work for a company called Recorded Future, and Recorded Future specializes in threat intelligence. My day-to-day job is to help our customers better integrate the flow of threat intelligence into their processes. Often times, people will have threat intelligence sitting in one bucket and then they'll have their logs from their different devices sitting in another bucket, or in multiple buckets.

The threat intelligence isn't necessarily providing them immediate and actionable value. To me, that makes it not really threat intelligence. That makes it interesting information, but until you can actually apply it and automate it in a regular way, it's not that intelligent. That's kind of what I do on a day-to-day basis.

Then, separately from that, Tim and I talk several times a month just — I don't want to say mentor, because we've both been in the industry the same amount of time, but we have a lot of ideas, share a lot of ideas and kind of work together, and I highly encourage that in the industry to find people that you know and just call them up and talk about security stuff sometimes. It's often better than chatting with your family about it, because they don't roll their eyes.

[0:51:01.9] TG: Yeah, my day-to-day is — I'm a cyber-security specialist at Semantics. My day-to-day involves working with our customers to talk about looking at their holistic cyber defense platforms; what are they doing for cloud-to-core monitoring and engagements of their systems to be able to do log analytics, incident response, and assessing their overall incident response programs, plans, and playbooks. Also, working with their threat intelligence teams if they have dedicated threat intelligence teams to help them better understand and implement operational as well as strategic intelligence practices to move towards an intel-guided network and information defense system.

I find myself working with customers and talking a lot about what it is that they're doing from an operation's perspective. What it is that they're doing to provide better defenses in their networks and looking at their holistic security architecture and the operations that underpin it and help them find ways that they can better at it.

[0:52:02.1] JM: All right guys. It's been a pleasure talking to you about ransonware, and I'm following your work closely. I was really entertained and amused, or intrigued I think is the right word, when I was going through some of the material that you have both prepared. Thanks for coming on Software Engineering Daily.

[0:52:20.7] AL: Thank you so much for having us.

[0:52:21.0] TG: Thank you.

[0:52:22.3] AL: We really appreciate the great work you're doing; keeping people informed on just such a wide variety of topics.

[0:52:29.7] JM: You're very welcome.

[END OF INTERVIEW]

[0:52:34.6] JM: Thanks to Symphono for sponsoring Software Engineering Daily. Symphono is a custom engineering shop where senior engineers tackle big tech challenges while learning from each other. Check it out at symphono.com/sedaily. That's symphono.com/sedaily.

Thanks again Symphono for being a sponsor of Software Engineering Daily for almost a year now. Your continued support allows us to deliver this content to the listeners on a regular basis.

[END]