EPISODE 576

[INTRODUCTION]

[0:00:00.3] JM: Last year, the WannaCry ransomware attack shut down hospitals, public transportation systems and governments demanding payment to unlock key computer systems. A programmer named Marcus Hutchins was able to stop WannaCry by registering a DNS entry buried in the WannaCry code.

Not long after he stopped the WannaCry attack, Marcus Hutchins was arrested at a security conference in Las Vegas. Marcus's arrest was due to actions that were unrelated to WannaCry. He is accused of writing a piece of malware called Kronos. Marcus volunteered his time to help stop WannaCry. This was a piece of ransomware that threatened to cause billions of dollars in damages. Whether or not he was a black hat in the past, perhaps Marcus should be absolved of his past actions.

Reeves Wiedeman is a journalist with New York Magazine and he joins the show to tell the story of WannaCry's Gray Hat, Marcus Hutchins.

[SPONSOR MESSAGE]

[0:01:07.0] JM: The octopus, a sea creature known for its intelligence and flexibility. Octopus Deploy, a friendly deployment automation tool for deploying applications like .NET apps, Java apps and more. Ask any developer and they'll tell you that it's never fun pushing code at 5 p.m. on a Friday and then crossing your fingers hoping for the best. We've all been there. We've all done that. That's where Octopus Deploy comes into the picture.

Octopus Deploy is a friendly deployment automation tool taking over where your build or CI server ends. Use Octopus to promote releases on-prem or to the cloud. Octopus integrates with your existing build pipeline, TFS and VSTS, Bamboo, Team City and Jenkins. It integrates with AWS, Azure and on-prem environments. You can reliably and repeatedly deploy your .NET and Java apps and more. If you can package it, Octopus can deploy it.

It’s quick and easy to install and you can just go to octopus.com to trial Octopus free for 45 days. That’s octopus.com, O-C-T-O-P-U-S.com.
[INTERVIEW]

[0:02:38.3] JM: Reeves Weideman is a journalist with New York Magazine. Reeves, welcome to Software Engineering Daily.

[0:02:43.0] RW: Thanks for having me.

[0:02:44.7] JM: You are a journalist. You're not a software engineer. Most of the guests on the podcast are software engineers, but occasionally we like to do interviews of varying topics and this subject that we're going to discuss today is related to software engineering. It's a story about a gray hat hacker associated with the WannaCry ransomware attack. Why don't you explain the circumstances of the story that we're about to dive into?

[0:03:14.3] RW: Sure. Yeah, and I hope as someone who's not a software engineer that I don't say too many things that are embarrassingly stupid when it comes to describing the technical details of things, but I'll do my best.

The story we that we wrote about was about Marcus Hutchins. Marcus back in 2017 was he had just started working as a cybersecurity researcher, he's 23-years-old, living in England. At the time, he was living and working from his parents’ home in the rural UK. In May of 2017, a large ransomware attack, the WannaCry attack was hitting systems really around the world. One of the biggest targets was the UK's health system. It was taking a lot of hospitals offline, it was also attacking businesses throughout Europe and the rest of the world.

Basically, Marcus just jumped into action on his own time. It wasn't necessarily part of his job, like many people had done that day, because this was such a huge attack. Long story short, he basically – he's someone who do often tracks these type of attacks and he took a look at the code which was being passed around and found that there appeared to him to be a way for him to track what the botnets, or what the ransomware was doing by sink-holing the traffic.

He registered this domain name that he found in the code. When he did that, more or less by accident figured out that he had actually stopped the attack from spreading. He became this momentary hero both in the cybersecurity world and then more generally, now the BBC was at his house, reporters throughout the UK we're at his house, many really became this hero.

Then several months later, he came to the United States for a conference, the DEFCON conference in Las Vegas and as he was preparing to leave, he was arrested by federal agents in the United States. Who it was later revealed in an indictment were charging him with creating a separate piece of malware called Kronos, that had been created several years before, was completely unrelated to WannaCry, but according to prosecutors was something that Hutchins when he was younger had done.

Fast forward to us working on this article and today Marcus is awaiting trial, and/or his proceedings are ongoing. He has maintained his innocence. The question we were trying to do when in addition to trying to sort out was what was going on is how society should react to people in the computer security world, who on the one hand may be good guys, on the other hand perhaps when they were younger, learned some of their skills by mucking around in things they shouldn't have done. That is a long-winded way of explaining what the article is about.

[0:06:15.0] JM: Right, and I'm glad you gave such a detailed synopsis there, because there's a lot of different things that I would love to explore with you. Obviously, the contemporary aspect of hacking in terms of ransomware, ransomware is I think a somewhat new brand of malware. We've done a show on ransomware in the past, so people can listen back to that if they want a detailed explanation.

Ransomware is essentially malware that locks your computer up and demands that you pay money to a certain address, oftentimes paid in Bitcoin, or some other cryptocurrency. Once you pay, you get to unlock your computer. This attack vector is it's pretty strong, and there's a lot of different brands of ransomware that are attacking people throughout the world. WannaCry was particularly painful, because it was so widespread and it hit facilities like hospitals.

The other aspects that I want to explore aside from ransomware are of course, Marcus Hutchins himself. He's quite an interesting character. I'd to unpack the character of Marcus Hutchins and

I'd also to talk about journalism, because I think the world of journalism and software, there's increasing overlap there and there is a disconnect between those two areas. I encounter this disconnect all the time, because I'm a software journalist myself. Maybe we could start with the topic of journalism. Why did you write the story? What drew you into the story of Marcus Hutchins and WannaCry?

[0:07:54.4] RW: Yeah, I think we were interested in finding out who Marcus was, because I think he is clearly one in a cohort of people that are becoming more and more influential in society, which is people who work in cybersecurity. Ten years ago, maybe even five years ago, the work Marcus does didn't exist. Yet now, as it's becoming obvious in in many, many ways. People like him are more and more important, and more and more powerful frankly, in terms of what they can do, and in terms of protecting the internet, or potentially using their skills for harm.

I think a lot of lay people are scared, because they don't know this is such unfamiliar territory and most people would prefer to just imagine that technology just works – it just always works and we're always going to be safe and you don't have to worry about the sort of what's under girding it. I think people are becoming more and more aware that there are human beings who make these things work.

I think for us, it was just a chance to find out what someone from that world is like, who is Marcus, what kind of person is attracted to this work and then how do they react to very young ages and a lot of cases having a lot of influence.

[0:09:14.5] JM: I have done a couple interviews with Adrian Lamo, who unfortunately passed away recently. When he was pretty young, I think a late teenager, he started finding backdoors into websites like banks and I think The New York Times, all of these poorly designed websites in the late 90s. He would find these vulnerabilities and then he would e-mail the companies that hey, you have this vulnerability.

I think one of the companies ended up pursuing legal action against him, because he just notified them of their vulnerability. It was the first in a number of tragic events in his life, where he from my point of view is very clear, he was he was guided by pure morals and he had the best intentions at heart. Maybe early on in his career, he didn't really have the diplomacy to

really approach these issues correctly. I think similarly with Marcus Hutchins, you see somebody who started off in his career making some malware that maybe he later regretted, or maybe not, who knows; we can get into that.

You see this pattern with people who often start off just they're either curious, or they see the leverage that they can have with cybersecurity if they are some kid with a computer and they learn they can make a lot of money by hacking into certain systems. Then later on they realize, “Oh, actually with great power comes great responsibility. I probably shouldn't do that.” They change their tune, but their history follows them, and they are judged on their past actions. It seems like a theme among hackers. I mean, and you're reporting on this story, did you find more cybersecurity researchers that had that history, where they started off with as a black hat and then had a change of tune?

[0:11:06.7] RW: Yeah, I think it's a trope in cybersecurity that everyone has a past. There is some truth to that and I think there's some exaggeration. I think, again it's one of those things where you and choosing your words there, like hacker has a negative connotation. Whereas, in this world it very much doesn’t.

I think that there's two things. I mean, I think I think there's a lot of hackers who, when they're teens figuring out how to program for the first time and figuring out what they can do, I don't think many of them would identify as black hats, but I think at the same time they're going to test the limits of their skills, and it's also happening at a point just developmentally when people had age don't have a perfect moral compass in a lot of ways.

In some cases, teenagers in years gone by might have egged a house, a teenager now might decide to deface a website, and they might not see it as like, “I'm a bad guy and I'm doing bad,” they're just doing harmless pranks. Now there are some people, and there's at least allegations that Marcus was someone who was maybe doing even more than that. Then then we get into even more difficult area.

It's certainly the case that one thing we have to deal with is that some of the best people in this field are young and in their not distant past they might have done things that, yeah, they shouldn't have. Then it falls on companies who employ these people, or governments who might

employ them, or work with them, or consider prosecutions against them, to determine what is in the broader interest of securing the internet.

[SPONSOR MESSAGE]

[0:12:57.7] JM: Azure Container Service simplifies the deployment, management and operations of Kubernetes. Eliminate the complicated planning and deployment of fully orchestrated containerized applications with Kubernetes.
You can quickly provision clusters to be up and running in no time, while simplifying your monitoring and cluster management through auto upgrades and a built-in operations console. Avoid being locked-in to any one vendor or resource. You can continue to work with the tools that you already know, so just helm and move applications to any Kubernetes deployment.

Integrate with your choice of container registry, including Azure container registry. Also, quickly and efficiently scale to maximize your resource utilization without having to take your applications offline. Isolate your application from infrastructure failures and transparently scale the underlying infrastructure to meet growing demands, all while increasing the security, reliability and availability of critical business workloads with Azure.

To learn more about Azure Container Service and other Azure services, as well as receive a free e-book by Brendan Burns, go to aka.ms/sedaily. Brendan Burns is the creator of Kubernetes and his e-book is about some of the distributed systems design lessons that he has learned building Kubernetes.

That e-book is available at aka.ms/sedaily.

[INTERVIEW CONTINUED]

[0:14:33.0] JM: Marcus Hutchins was able to stop WannaCry. What was the background of Marcus Hutchins prior to WannaCry? Give some more details on that.

[0:14:43.4] RW: Sure. Marcus had – he had gone to school for a while, he had had taken a two-year college course, set of courses in the UK. Then was struggling to figure out what he wanted

to do. Cyber security for one thing is not the easiest industry to get into, in part because it's changing so fast, and part because people don't know exactly what the jobs are.

I think for a good while, he in his very early 20s, he was trying to figure out in what way his skills could be useful. At one point, he decided to start a blog called malwaretech.com, which was his handle prior to him stopping WannaCry. No one really knew who his name was, even people he was close to online. He's just blogging about the work he was doing, mostly tracking botnets.

At a certain point, employer in the US, at a cybersecurity firm called Kryptos Logic read a post that Marcus had written about a particular botnet was impressed with his work, reached out to him and gave him a trial position at his company, and eventually a full-time one. At the point that Marcus stopped WannaCry, he'd been working at this company, I think for a year, year and a half.

At that point, as a full-time cybersecurity researcher, at a very good salary, and he was someone who by that point had become reasonably well-respected. He wasn't he wasn't famous by any stretch, but people who did this work knew who he was and by and large I think, respected the work he was doing.

[0:16:23.7] JM: When WannaCry occurred, governments and companies were affected by it. Maybe you could just give another brief breakdown of the events that led up to WannaCry and it spread throughout the world and how Marcus responded to the events of WannaCry?

[0:16:45.3] RW: Yeah, sure. Basically this one day in May, people were arriving at their places of work and finding that they were locked out of their computers by some piece of ransomware. People had varying levels of knowledge about what was happening. That was telling them that if they wanted to access their computers and the files on their computers, they needed to pay a ransom.

This happened to British hospitals, a telecom company in Spain, the Romanian Ministry of Foreign Affairs, police departments in India, organizations all across the world were getting hit. Cyber security is this field where a lot of the people who work in it, they do it for fun. They

obviously do their jobs to get paid, but it's also in a lot of cases their hobby and something they like doing.

Marcus and a number of other people saw this was happening, and it wasn't necessarily Marcus's job to try to do something like this, but he and others basically got a sample of the WannaCry code and began looking at it. What Marcus noticed was that there was – in the code, there was this random domain name. It was 25, or so numbers and letters seemingly in a random order dot-com, that was in the code and he noticed that it was unregistered.

In many cases with pieces of malware, they'll have these unregistered domain names, basically as a way to so that the – again, this is where I'm pushing up against my knowledge, but often these pieces of malware will be designed so that they will be communicating to this unregistered domain name. If that domain name ends up being registered, the malware will know that it's been trapped in a sinkhole.

Marcus uses that, has in many cases he told me he'd done this probably hundreds of times; registered that domain name, basically as a way to then track the malware. Because it communicates back to this domain name, he thought that if he had registered it, he would be able to see where it was – where it was going and just get a picture what was happening.

What ended up happening is that when registered the domain name, he basically activated what was then called a kill switch that just stopped it from spreading. By that point, there had been considerable damage, dozens of hospitals in the UK had been closed, significant amount of money had been lost just in terms of lost business around the world, but once Marcus hit that kill switch, by and large the malware stopped propagating. It didn't spread further.

[0:19:27.8] JM: Shortly after this attack was halted, and Marcus became this international hero essentially. He later found himself at a conference, as you mentioned in Las Vegas and he was arrested at that conference. He was arrested, because he purportedly had created this software in the past called Kronos. Explain what did he do in the past? What was this software Kronos? Why was it so malicious?

[0:20:02.7] RW: Well, I should emphasize first off, that he's alleged to have done this. He of course –

[0:20:06.9] JM: Alleged, right.

[0:20:07.6] RW: - claims that he is innocent. What Kronos was, was it what's known as a banking [inaudible 0:20:12.1]. Basically, if Kronos was installed on your computer and you went to bankofamerica.com or whatever banking website you might use and put in your username and password, Kronos would surreptitiously take that information and would have it.

Kronos was a piece of malware that was people had spotted back in 2014 and was when it first emerged. It was being sold on Alpha Bay, which is a dark web marketplace, where people will often buy – cyber criminals will buy pieces of malware to then use. It never really became a huge problem, because obviously it was intended to do bad things. It certainly seems to have done that in some cases, but it was never the biggest threat. In fact, some people I talked to in cybersecurity said when this news broke about Marcus being involved, they had to go look up what Kronos was, because they couldn't even remember it.

[0:21:11.3] JM: Why do you think this happened? Did the FBI – how did they connect Marcus Hutchins to Kronos? Hid he just rise to prominence and then they're like, “Let's just start to investigate further who this guy is.” Then through their, I don't know, maybe there Palantir knowledge graph, they found out that he was the creator of Kronos. How did the FBI connect him to Kronos, and was there some mapping between Marcus Hutchinson's rise to prominence and this past alleged miscreants?

[0:21:42.9] RW: It's hard to say exactly why they decided to bring the prosecution. Of course, they are not obligated and haven't thus far said why. Some people believe it's because Marcus became a prominent target, but in terms of the evidence, they have revealed there are, at least the FBI says that there are chat logs in which Marcus discusses working on Kronos and talks about selling it on these marketplaces.

There was a confidential informant who the FBI was working with, who had purchased the malware. There is also, I should say a co-conspirator who was yet to be named by the

prosecutors who that person is the person who allegedly sold the malware allegedly after Marcus created it.

There does appear to be forensic evidence. A lot of people did tell me that the FBI doesn't bring cases lightly. At the same time, there have been – these are difficult crimes to prove, because of just the nature of data being quickly produced and quickly deleted, just the nature of how these things work. There's still I think a lot of questions to be answered about what evidence there is and why the prosecution was brought in the first place.

[0:23:00.8] JM: Marcus is denying he created it?

[0:23:02.7] RW: He is. Yes.

[0:23:03.7] JM: After Marcus was arrested, the public perception of him changed. Some people suspected him of potentially even creating WannaCry in the first place. Do people still suspect him of that, or how widespread is that allegation?

[0:23:23.2] RW: I think that's a pretty fringe view of things. I mean, the American government for one thing has said – it's among others have said that it was North Korea. I'd say that's a very fringe opinion at this point.

[0:23:38.4] JM: Yeah, about that North Korea, did you look into that any further about how the United States has figured out that it was North Korea?

[0:23:46.1] RW: I did not. That wasn't really something that we needed to spend our time on, but plenty of other people have reported that and governments around the world have done it. Unless, there's a widespread cover-up, it seems pretty likely at this point that that was the case in terms of who was behind that.

[0:24:06.0] JM: Yeah. There were some other criticisms of past actions that Marcus had taken when he was coming up as a teenage programmer. What else had Marcus done in his early years as a programmer that he was getting criticized for?

[0:24:25.1] RW: Yeah, basically what happened is a month or so after he was arrested, Brian Krebs who's a journalist who covers cybersecurity pretty much full-time, he published an investigation in which he had more or less convincingly connected Marcus to a variety of online usernames from the past, going back to when he was 14, 15 years old.

Some of the things that he was accused of were pretty low-level cybercrime. It wasn't exactly stuff you want to be doing, but it's stuff that I think a lot of teens his age do to one degree or another, it just depends on how far you push it. Some of the usernames, at least that Krebs had had found and that he believed he could tie to Marcus had designed these programs that could steal passwords, or there was one YouTube video explaining how to use a particular piece of malware.

Even Brian Krebs, who when you're talking earlier about journalism and cyber security, he's about as good as it gets in that particular field. He acknowledged A, that he couldn't connect Marcus to Kronos in any way. That the crimes were relatively small time in the scheme of things.

What it did, I think was served to show a little bit of a potential pattern of behavior, and it resulted in two reactions. Some people were very quick to condemn Marcus, and I think other people were very quick to say his history is not that different than mine, and that, yeah, a lot of people – I think a lot of people saw themselves in Marcus.

[0:26:02.4] JM: Well, God bless Brian Krebs. He's one of my favorite journalists. Did you get to talk to Brian Krebs for the story?

[0:26:09.2] RW: I did not. No.

[0:26:10.1] JM: He's elusive.

[0:26:10.8] RW: Yeah.

[0:26:11.7] JM: I've been trying to get him on the podcast for a while. If anybody out there is listening and they know Brian Krebs, maybe you can send him my way. Did you learn anything about how the FBI interacts with people who have committed cyber – I have this image, it's

romanticized, but I think it comes from the stories of the 90s and hearing about Kevin Mitnick and some of these other famous hackers.

This image of the FBI arrests somebody and then maybe they spend a little time in jail and then they get turned and then they become an advocate for cybersecurity, or they join a consultancy, or they start their own consultancy, there's this turning process that the FBI instigates. Did you get any insight into how the FBI tends to interact with these black hat or gray hat programmers?

[0:27:09.2] RW: Well, I think a number of people who've either worked for law enforcement, or otherwise suggested to me. Yeah, the FBI is not looking in general to crack down on small-time cyber criminals. They're looking to catch big fish. There have been cases in the past, where yeah, they've caught someone doing smaller time and used them, but that's the case in any crime.

I do think there's a genuine effort on the part of law enforcement to create better relationships with the hacking community. Certainly the Department of Justice has put in a lot of initiatives to do that for a number of reasons; one, the government needs cybersecurity people as much as anyone else and they need the private sector, cybersecurity world is just as important in terms of protecting various government systems and private systems.

I think there's a genuine effort on the part of the DOJ and other government agencies to build better relationships. I think the potential issues that something like Marcus's case, where he was very clearly considered a hero for to a lot of people in this world, to then see him get arrested for something makes a lot of other people wary and just inherently distrustful and this is in a community that is probably by nature more distrustful than most of authority and the government. We don't know to what extent the prosecutors considered the broader implications of this, but it's at least something that seems worth keeping in mind.

[0:28:51.7] JM: What is the state of Marcus Hutchinson's life right now in his case?

[0:28:57.9] RW: He's still stuck living in the United States. He can't leave. He is living in Los Angeles and his lawyers and the government's lawyers are basically locked in a battle of competing motions on a variety of things, the trial. I think there's really no dates in place.

A lot of these cases do end up in in settlements, so that seems at least possible. At this point, he's just letting the legal proceedings go, because there isn't too much else for him to do. I think no one fully knows exactly what's going to happen, but that will play out in the coming weeks and more likely months ahead.

[SPONSOR MESSAGE]

[0:29:45.8] JM: Software workflows are different at every company. Product development, design and engineering teams each see things differently. These different teams need to collaborate with each other, but they also need to be able to be creative and productive on their own terms.

Airtable allows software teams to design their own unique workflows. Airtable enables the creativity and engineering at companies like Tesla, Slack, Airbnb and Medium. Airtable is hiring creative engineers who believe in the importance of open-ended platforms that empower human creativity.

The mission of Airtable is to give everyone the power to create their own software workflows; from magazine editors building out their own content planning systems, to product managers building feature roadmaps, to managers managing livestock and inventory. Teams at companies like Conde Nast, Airbnb and WeWork can build their own custom database applications with the ease of using a spreadsheet.

If you haven't used Airtable before, try it out. If you have used it, you will understand why it is so popular. I'm sure you have a workflow that would be easier to manage if it were on Airtable. It's easy to get started with Airtable, but as you get more experience with it, you will see how flexible and powerful it is.

Check out jobs at Airtable by going to airtable.com/sedaily. Airtable is a uniquely challenging product to build, and they are looking for creative front-end and back-end engineers to design systems on first principles, like a real-time sync layer, collaborative undo model, formulas engine, visual revision history and more.

On the outside, you'll build user interfaces that are elegant and highly customizable that encourage exploration and that earn the trust of users through intuitive thoughtful interactions. Learn more about Airtable opportunities at airtable.com/sedaily.

Thanks to Airtable for being a new sponsor of Software Engineering Daily and for building an innovative new product that enables all kinds of industries to be more creative.

[INTERVIEW CONTINUED]

[0:32:05.4] JM: When I was looking through the story, I was also looking through the other stories you've written recently, and it's quite a mix of different topics that you explore. A lot of the technology journalists that I talked to on the show, when we do shows with journalists, when we're not doing shows with software engineers, their focus, their entire focus is technology, like what stories can be covered in technology. Your focus is not exclusively technology. Is there some theme in the stories that you try to explore?

[0:32:39.9] RW: That's a good question. I think the thing that probably connects it and connects Marcus to some of the other stories is that I'm interested in writing about people who are in interesting positions, and Marcus has certainly found himself in that case just based on everything that he has done and what has happened to him.

I think he was just an interesting person to get to know as something of a stand-in for I think this broader demographic of people that as I mentioned earlier are just becoming more and more important.

Frankly, I think for our purposes, it's not necessarily getting into the technical nitty-gritty, but we just wanted to find out more about Marcus as a person, and as a way of finding out more about this group of people.

[0:33:26.7] JM: Another long-form piece that you wrote recently was about Uber. Describe what was the nature of the story you're writing about Uber?

[0:33:36.0] RW: I was doing a piece, more or less about the difficulties that company was going through. This was roughly a year ago. At the time, they were dealing with just a seemingly endless string of bad press; from their founder getting in trouble, saying things he shouldn't have said, to issues with sexual harassment and other workplace issues to just business problems.

I think people realizing that the company was in trouble, at least potentially, it wasn't just this obvious rocket ship of a company. I think, maybe for your listeners interests, I was spending a lot of time talking to engineers at the time at the company who had worked there, or either had been there or were still there, and just trying to get a sense of what it was like to work at this company that was constantly coming under fire and that you consistently had to explain to your friends, even though the work you were doing was really interesting, you were having to explain these why you were working for this company that was seemingly found itself having bad press all the time. Yeah, it was just an overview of that, of where Uber stood at that point.

[0:34:50.0] JM: Yeah, what's your sense for how the ride-sharing battle will play out? Do you think that Uber can escape the subsidy-based business that they're in right now?

[0:35:01.8] RW: My sense of it was I think that certainly, the service that Uber and Lyft and many others provide is one that many, many people find very useful. It's a service that's going to exist. It's less clear to me that that Uber, or any of those other companies is going to completely transform all modes of transportation and be worth tens of billions of dollars. I think, at some point they're not going to be able to completely subsidize these rides.

I think the rides will probably end up getting more expensive, and I think there may not be a bad result for Uber being a national taxi cab. That's not a world-changing business, but it's a really good business and I could imagine them settling into that. I think a lot of the problems that we talked about in that story a year ago are ones they still face and are still dealing with.

[0:35:52.6] JM: Another recent piece that you wrote recently was about Exxon and the Rockefellers. I wanted to ask you, how do you feel about the difference between the history of big oil and that of big technology that we're starting to see rise to prominence today? Do you see any parallels between those two gigantic industries?

[0:36:18.9] RW: First thought that comes to mind and I might direct your listeners to the latest issue of New York Magazine, as we just did a piece about people from a variety of tech companies is coming to terms with what they have wrought on society, and that a lot of these big companies have had effects that were unintended. Some, I think have been negative.

I think, for certainly I'm not sure that Big Oil ever had the savior complex that a lot of people in the tech world, I think have. Certainly early on in the oil boom and one thing that Exxon and other energy companies will say is, “We're making people's livelihoods better by providing cheap energy and that whatever consequences there are two that are worth it.”

I think in in the same way that people in the tech world are coming to terms with it with that a little bit, and having something of a reckoning, I would say that's probably the case for at least the more introspective people who work in the energy world.

[0:37:24.1] JM: Tell me a little bit more about that piece, the Exxon and the Rockefellers, what were you covering there?

[0:37:28.2] RW: The Rockefeller family, which has all of its money from standard oil, which eventually became Exxon, a number of members from that family have tried to push Exxon to come to grips with climate change and the companies effect on that. The piece was covering for the battle between those two sides. Exxon has pushed back against the Rockefellers, the Rockefellers have gotten a certain amount of attention, because of their family history to this problem. They're currently locked in a bit of a legal battle that they've been roped into with several states attorneys general, including in New York, Massachusetts who are considering a probe of Exxon and what the company knew about climate change at various points in its history, versus what it said publicly.

The case is in some ways has similarities to the tobacco cases, where the tobacco companies knew the consequences of smoking and purposefully obfuscated that. In Exxon's case, there at least to some evidence that the company's executives were well aware of climate change and their role in it and the potential of negative consequences, but that publicly were much more likely to decide not to talk about that, at the very least.

[0:38:46.5] JM: As we wrap-up, I do want to talk a little bit about journalism and your perspective on it, your trajectory in journalism. On the show, we've had people from larger journalistic institutions; Bloomberg, New York Times, New York Magazine of course such as yourself and then we've also had people who are individual journalists, who are building their own brand, striking out on their own, or being medium authors, or bloggers or podcasters.

When you look at this spectrum of journalistic opportunities, how are you charting your course? Are you focused on just producing extremely good content and finding a publisher where you can house yourself? Or do you see a brand to build for yourself? What's your trajectory?

[0:39:39.0] RW: Well, I work full-time at New York Magazine and more or less do feature stories for the magazine and very happy doing it. I think freelancing is a tough game. I think Brian Krebs is a great example of someone who's really managed to do that. I hope, well I don't know anything about his finances, but he does seem to have built a career on his own, which I think is really admirable.
I think it's tough to get into that. I think freelance writing is a side thing if you like it, or to – in Marcus's case, he just started the blog and that helped him get a career doing something else. I think that's a really, really admirable thing and really, really good way to go about it. For me, I'm working at New York Magazine and much more interested in just doing good work for the magazine than promoting my own brand at this point.

[0:40:24.9] JM: What story are you working on now?

[0:40:26.7] RW: Another story about a company that's going through some difficulties. That's what I'm working on right now.

[0:40:33.7] JM: Okay, well Reeves Wiedeman, I want to thank you for coming on Software Engineering Daily. It's been really great talking to you. Do you have any predictions for what else is going to come out in this WannaCry case?

[0:40:44.0] RW: I don't. I think the only thing I'll predict is that whatever result I think will have a big impact on the cybersecurity world. If Marcus is found guilty, I think that would obviously be a

big deal. If he's found innocent, or is let go, I think people have a lot of questions about the prosecution. Either way, I think it's a case to watch.

[0:41:03.7] JM: Okay. All right, well thank you for coming on the show once again.

[0:41:06.1] RW: No worries. Thank you.

[END OF INTERVIEW]

[0:41:10.6] JM: We are running an experiment to find out if Software Engineering Daily listeners are above average engineers. At triplebyte.com/sedaily you can take a quiz to help us gather data. I took the quiz and it covered a wide range of topics; general programming ability, a little security, a little system design. It was a nice short test to measure how my practical engineering skills have changed since I started this podcast.

I will admit that, though I've gotten better at talking about software engineering, I have definitely gotten worse at actually writing code and doing software engineering myself. If you want to take that quiz yourself, you can help us gather data and take that quiz at triplybyte.com/sedaily.

We have been running this experiment for a few weeks and I'm happy to report that Software Engineering Daily listeners are absolutely crushing it so far. Triplebyte has told me that everyone who has taken the test on average is three times more likely to be in their top bracket of quiz scores.

If you're looking for a job, Triplebyte is a great place to start your search, it fast-tracks you at hundreds of top tech companies. Triplebyte takes engineers seriously and does not waste their time, which is what I try to do with Software Engineering Daily myself. I recommend checking out triplebyte.com/sedaily. That's T-R-I-P-L-E-B-Y-T-E.com/sedaily. Triplebyte, byte as in 8-bytes.

Thanks to Triplebyte for being a sponsor of Software Engineering Daily. We appreciate it.

[END]