MYTH DEBUNKED: MY MAINFRAME CAN'T BE HACKED

BMC AMI Z Talk · Episode 3: Myth Debunked - My Mainframe Cannot Be Hacked

In this episode of BMC AMI Z Talk, security experts Grant McDonald and Chad Rikansrud from BMC expose the common myth that the mainframe cannot be hacked and share why it should be included in your enterprise security strategy. Below is a condensed transcript of our conversation.

Grant: So this is a topic that is near and dear to my heart and Chad's heart. I know he's done countless presentations on this at many events across Black Hat, DEF CON, SHARE, you name it – It's probably been something he's spoken. And you may have even heard him at one of those events – those of you that are listening. But for those who don't know, Chad, I wonder if you might start out by giving a little bit of the background – before we get into how a mainframe is hacked – kind of your journey into discovering that for yourself because I don't think you were always the mainframe hacking guru you are now, right?

Chad: Hey, Grant. No, I am not. Thanks for having me here. Nope, that is the case. In fact, I've only been doing mainframe, from a technical perspective, for maybe the last – I'll be generous here and say 12 or 13 years, which makes me positively a newb by mainframe standards where most of the people have 20, 30, 40 years of experience. So definitely did not grow up in mainframe.

But how I got here, to answer your question, I worked for a global financial institution. And I was running mainframe infrastructure for them – a lot of their storage and their ability to recover and all things data privacy and that sort of stuff. And one of the things that occurred to me – This was about the time that ransomware had become really in vogue, so maybe – I don't know – six, seven, eight

years ago.

It just occurred to me because I've always had a background in Linux and networking and security. And I was really fascinated by this idea of ransomware and how the bad guys of the world had now really figured out how to monetize their various behavior in a very, very efficient manner, which is ransomware.

And I got to thinking about well, I wonder who's doing the kind of research on the mainframe that would protect it from this sort of stuff. Because I was always fascinated by the people that – Microsoft releases a patch because somebody found a 0-day in a TCP/IP stack. And I'm like, man, that is just so cool. Who is doing this kind of research on the mainframe? And would it be susceptible to the types of things that we see that allow for something like ransomware, as an example, to happen?

And so I, having access to all kinds of resources because I worked for a giant bank – I just started poking at it and really teaching myself COS in the mainframe in order to get to the point where I could write exploits and testament stuff. And just to give you an idea of the undertaking there – and I don't mean this to toot my own horn. But it took me a couple years of heads-down, technical work on the mainframe to get to the point where I could even really start that. It would be the equivalent of learning to crawl so you could run a marathon. It was quite an undertaking.

But the punchline of the whole thing is ***it's just another computer***. And it's absolutely susceptible to all the types of vulnerabilities and attacks that all the other computers are. It's a computer operating system written by humans for humans. And as such, there are mistakes that are out there and misconfigurations and coding errors that can all be exploited. And so, I started figuring out how to do that and writing talks, as you mentioned, and tools and that sort of stuff to do that. And here we are.

Grant: Gotcha. You mentioned how it took you some time to get up to speed and understand the mainframe. Now, this is something I think that somebody on the other end, I could see, listening to this and say – Aha! See, it took you how long to get up to speed on the mainframe before you knew how to uncover all these compromises. Do you think it still would take somebody to really get that level of expertise in order to compromise a mainframe or is it simpler than that

Chad: Yeah. It takes a long time, and here's why. It's an operating system that is unlike any other operating system. It is not forgiving. There's no training wheels for it. There's no wizards or strips you can follow along with. There are attempts at that. But to really understand – For instance, if you want to write an exploit of something, you really have to understand how memory is organized and how programs are organized and how they work and how things are stored on disk.

If you get to that level, you have to first understand basic stuff on the operating system – how to install it, how to upgrade it. How does it boot? How does the load process work? All that. It's just a tremendous amount of information there – So, there's two things.

One, it's well-documented to the point where it's actually, I would say, over-documented. Everything is documented. There are tens and tens of thousands of pages of documentation, but none of it is presented in a way that is – so you want to exploit the mainframe. Here's what you need to know. You can go out and take a class on how to do that in Windows and have relatively little Window experience, and they will take you right to the head of the class of – Okay, here's the kernel, and here's how it works. And here's how drivers work. And here's how memory works. And so on and so forth.

That doesn't really exist for the mainframe. The classes and the stuff that's out there that exist for

DUS are really geared at people who want to learn how to develop programs for it or operate it or use it. But in terms of the people who want to do what I'm doing, which is find vulnerabilities and exploit them and learn how to pen test it and improve that discipline, that knowledge isn't really out there. We've been forging, by and large, an untested trail with the exception of a few people out there in the world who've done a little bit of this work, as well.

Grant: Gotcha. So do you think that, in part, is what gives credence to the belief sometimes that people feel the mainframe should not be regarded as part of their security plan because they feel it's this box in the back corner that doesn't really require the same controls as a Windows device?

To listen to the rest of this episode, visit SoundCloud or Apple Podcasts