MARCH 30, 2020

A Gamer’s Influence on DDoS

Presenter: Mary Haynes

> *“As these attacks grow, these attackers are finding new ways to warp ISPs protection mechanisms. And so it's a daily battle that we're fighting every day. But it gets really no publicity because in many cases, many of the service providers are protecting their customers and they don't even know it. We are putting a lot of dirty traffic out there because of these, in many times it's just gamers, trying to knock off another gamer and they don't realize the destruction they're causing.”*

Summary

For gamers and users heavily dependent on high-traffic internet platforms, loss of service is destructive--and can be symptomatic of a greater distributed denial-of-service (DDoS) attack. Charter Communications VP Mary Haynes goes in depth into its evolution over the years, tactics for mitigation, and how some gamers inadvertently end up worsening the situation.

Transcript

Brian Contos:

Welcome to the Cybersecurity Effectiveness Podcast, sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve, and communicate security effectiveness. I'm your host Brian Contos and we've got a really special guest today. Joining me is Mary Haynes. Welcome to the podcast, Mary.

Mary Haynes:

Thanks Brian. And thank you for creating this platform, highlighting women this year.

Brian Contos:

Oh, You're welcome. And I'm so excited to have the opportunity to do that and of course have you on the show. I've got a number of things I want to get to, especially around distributed denial-of-service attacks Mary. But before we get there, if you could give our listeners a little bit of background about you and the path you took to cyber and what exactly it is you do today?

Mary Haynes:

Sure will. So, Brian, today I work for Charter Communications. I lead a very large team that's focused on protecting the services we provide to our customers. Which include cable services, voice services, as well as high speed internet services. I've been in the field though for about 25 years, primarily in the telecommunications and cable industry. I was very fortunate to be working at AT&T before I got into security and through a leadership development program at AT&T. They were needing more women in technology. So, once I completed that program, they offered me an opportunity to move from the customer care organization, over into a technology job, and specifically in the network security organization.

Mary Haynes:

It's been such an amazing career, and I was very, very fortunate to be the first girl on the network security team at AT&T.

Brian Contos:

Really, number one? Good for you.

Mary Haynes:

I was number one and they actually hired me because I had a lot of Unix experience surprisingly enough.

Brian Contos:

Okay.

Mary Haynes:

This was before security tools were even available and they were concerned because we had deployed thousands of Unix servers and we needed someone to look at them to figure out, "Hmm. Are they being set up correctly and securely?"

Mary Haynes:

And so, we had to figure out and write some of the very first security auditing software, that audit things like windows, and then eventually Microsoft servers as well. So, it was a great way to get in. I've taken about every path in the security field since then. I've worked for several different telecommunications company and it finally got to a point where I'm actually leading a network security organization today at a fortune 100.

Brian Contos:

Wow. Wow. What an amazing path. A lot of people come up to me and they're like, "How do I get started in security, and what are some of the paths and system administration and network administration?" What you're in the IT field, there's always I think a good way to get your feet wet. But certainly, as you mentioned, those early days of auditing Unix systems and just hardening the operating system. You learn so much about, "Okay, let's get rid of the cleartext protocols and the all the R commands and privileges and group ownership" There's just so much you learn just by hardening a single system, you kind of get the feel for that. It gives you that great base—

Mary Haynes:

It does.

Brian Contos:

--By taking that path. Yeah. So, 25 years. Certainly, you've seen a lot of trends come and go. One of them that I know you're quite passionate about, and it's still around, DDoS, a Distributed Denial-of-Service attacks. Why are they so concerning today?

Mary Haynes:

Well, being in an internet service provider environment, it is a threat that we see happening every day. Matter of fact, in my network I see several thousand DDoS attacks against our customers every single day.

Brian Contos:

Wow!

Mary Haynes:

And I remember when DDoS first commercially hit. DDoS has been around since gospel. Actually, in the 70s is when the first person demonstrated that a DDoS attack could occur. But the first DDoS attack really kind of occurred in about 1996. And when that occurred, it was a SIEM flood attack, and it took down many services for days. It affected hardware vendors, mostly Cisco devices or Cisco themselves, because they didn't have the right defenses. There were no defenses except for shutting down network. And then when there was a DDoS attack, that was at DEF CON back in 1997, a guy at that conference demonstrated how DDoS worked.

Mary Haynes:

And then during that conference, the sample code was then used to actually launch an attack against Sprint, EarthLink and E*Trade. And having worked at AT&T at that point in time, we were very, very nervous about DDoS attacks. It's been interesting though to watch how DDoS attacks have evolved today. The latest thing in the news was, I think really back last year when an unknown service provider fell victim to what was considered the largest DDoS attack in history, which was about 1.7 terabytes per second.

Brian Contos:

Wow!

Mary Haynes:

And when I look at some of my customers today that use our services, they have these five gig links, seven gig links. This really could take down easily one of our customers, let alone many, many customers. And the reality is, in 2019 we actually are seeing DDoS attacks that exceed two terabytes per second on a daily basis.

Mary Haynes:

So, it is a continuing and growing problem. And what's interesting about this phenomenon. Actually, that attack, that last reported largest attack in the history, that US service provider actually shared with us. That was actually an attack against an elderly woman living in a mobile home—

Brian Contos:

Oh geez!

Mary Haynes:

—and the hacker attacked the wrong IP address. They were actually trying to attack the person that had the IP address last month. So, as these attacks grow, these attackers are finding new ways to warp ISPs protection mechanisms. And so it's a daily battle that we're fighting every day. But it gets really no publicity because in many cases, many of the service providers are protecting their customers and they don't even know it. We are putting a lot of dirty traffic out there because of these, in many times it's just gamers, trying to knock off another gamer and they don't realize the destruction they're causing.

Mary Haynes:

But there's going to become a point in time where the ISPs won't be able to stay ahead. And I keep thinking about, "Oh my gosh! If I was a nation state, what a great way to affect a country. If I can take down the key service provider's networks, what would be the impact to our critical infrastructure and all of the critical infrastructure structures that rely on our network to provide their services?"

Mary Haynes:

From a service provider's standpoint, it's one of the top three threats that we think exists in the marketplace today. But it's also one of the least talked about threats today. So that's why I find it so interesting. It's something I follow on a daily basis. My team's always trying to stay ahead of what the bad guys are doing. Our vendors that help us provide the services to do the protection are having a difficult time staying ahead of this phenomenon.

Mary Haynes:

And I think it's just going to grow and grow and grow and everyone depends on our network. They say energy is the most important critical infrastructure, and we're obviously seeing the impacts as utility companies are shutting off electrical services to prevent fires, et cetera. But network is actually your second most critical infrastructure. And I actually believe DDoS is the thing that could cause the greatest impact someday in the future.

Brian Contos:

Yeah. I think those are really interesting perspectives. I'm trying to think back to my first experiences with it and I think it was probably the Ping of Death, which you're probably familiar with that as well. ICMP: echo request 3, and, "Oh, I'm getting overloaded."

Mary Haynes:

Mm-hmm.

Brian Contos:

More of a nuisance than anything else at that point. And I think the motivations back then were more of curiosity or maybe just somebody was disgruntled and wanting to get a little bit of revenge. You mentioned some other core motivations there. They might be tied to nation states that are definitely up to something more nefarious or maybe not even a nation state, but some type of politically motivated group. Whatever that might be, terrorist organization, et cetera, et cetera. Let your mind explore that.

Brian Contos:

You also mentioned gamers knocking each other off, and in doing so, instead of just taking the car off the freeway, they kind of blow up the whole freeway. What are you seeing as some of the prime motivations behind this? Is it people that are still going after some kind of... Are they holding people for ransom? "Look, I just took you off the net. If you don't pay me X, I'm going to do it again." Are you seeing a lot of nation state involvement in this? and maybe there's some things you can and cannot share at your level. From a telecom perspective, what are some of the most common motivations or drivers behind these DDoS attacks?

Mary Haynes:

Well, the number one is actually the gamers. And they don't really realize what they're doing. They only see the immediate gain, right? "That I'm playing a game, I've captured your IP address." And you know, these tools are easily available on the internet and you can watch a short film on YouTube, quickly figure out how to knock that person off the game. And that really is today about 90% of the DDoS attacks that occur today across our networks.

Brian Contos:

Mm-hmm.

Mary Haynes:

But at what we're actually seeing, probably for about the last six years or so, is the hacktivism. Ferguson, Missouri, back about five years ago, if you recall, there was a lot of hacktivism going on after when the police inadvertently shot a young African American gentleman. And we saw a lot of hacktivism primarily using DDoS attacks against our government facilities, et cetera. And we're continuing to see that with Anonymous and some of these other threat groups.

Mary Haynes:

As far as nation States, right now I think they're really depending on our networks to do the other things that they're doing today. We actually though, do find a lot of different threats and bad things that nation States are doing and we're actually a theater to a lot of the intel that occurs with our government agencies about what we're seeing them doing. But right now they pretty much rely on the networks for staying up. But we're seeing now, countries trying to figure out how to disconnect from the internet when there is a potential nation threat against their country. I think we'll probably pursue that at some point here in the US as well.

Mary Haynes:

There's been talks about “how do I push the red button to shut down the internet to protect the United States?” And I think we're just preparing so that when that day comes, we have that ability to protect at least our infrastructure and communications here in the US. Again, like I said, it's so important, everything we do today. It's funny being in this business, I remember 20 years ago, if the internet went down, you rarely got a call about it. People didn't really even notice. Now if we lose our DNS for even 30 seconds, we have thousands of customers calling, screaming because we've become so dependent on those services.

Mary Haynes:

And I think they'll begin to realize, "Hey, if I'm going to attack them, especially if there's a coordinated attack, attack the network, attack the physical ability, and you've really held a country at ransom at that point in time." So, there's a lot of talk about what we can be doing in the future and a lot of testing going on in the background to prepare ourselves when that day comes. But we are just wondering when that day will come at this point.

Brian Contos:

Let's talk a little bit about that, then. Maybe you could give a couple of examples. One example from maybe a smaller mid-size organization. What can they do to help address this? And then potentially from the size of a larger organization, a large financial or a large telecom or even a government organization. Somebody with a little bit more financial might a little bit more horsepower behind them. And maybe they take the same approaches, I don't know. But what can organizations do today to help mitigate this threat?

Mary Haynes:

Well, I think you're a small organization, which actually fits the profile for most of our businesses here in the US. You really need to work with your service provider and figure out what managed security services they have specifically to prevent them for DDoS attacks. Most of the service providers do offer their business customers a service to protect themselves from this threat. They use their own protections that we use to protect our own network. Then we turn around and use those same services to also protect the end customer, which is a win-win for everybody at that point.

Mary Haynes:

I always say that's the number one place to start. We're also seeing again, along with that, just in general for security. But I think small business owners are realizing the need to utilize managed security services because they don't have the staff or the people or even the expertise to know how to protect their business.

Mary Haynes:

This is one of those first services they probably should look at, that really can be one of their first worries to get off their plate because they can get that from probably whoever's providing their network services today. For mid-size businesses that really do run their own network or have control around at least the perimeter of their network, then the very first thing you need to do is drop all the services you don't need. Most of the DDoS attacks today and over the past 10 years, use some very common protocols that really shouldn't be coming into your network. Things like

SSDP, that's a LAN protocol that's used for gaming. Really shouldn't be coming from the external perimeter of your corporate network. Old protocols like charging, Quote of the Day. Again, that's stuff that should only be internal for your network. If you even use those kinds of services, that are kind of tied to the old mainframe stuff, et cetera.

Brian Contos:

I was going to say. Are you still seeing that out there? The old character generation and all that?

Mary Haynes:

We are. These old tools are still out there. They're still using the protocols. And I'm just so amazed that there are still a lot of networks that are open for this type of protocol.

Brian Contos:

Wow!

Mary Haynes:

And then, there's things that you can also do around common protocols that you have to use. Like NTP. A lot of businesses rely on getting NTP from an external time server and there are certain packets that you really shouldn't be allowing in that are used for NTP amplification attacks. And you should be limiting your UDP traffic. Because that's a signal as protocol, right? It's not getting that ARC return.

Mary Haynes:

UDP flooding is something we still see a lot of because people aren't rate-limiting their UDP traffic. So there's a lot of good white papers out there, that describe the protocols everybody should drop. Those are kind of the protocols most service providers put on the outside of their networks as well, and don't even let it go. And then if you're a large organization, you really do need to be talking to a DDoS service provider. There are some great solutions out there that ISPs use today. Many of those same vendors provide very affordable offerings as far as a cloud service. And so if you're a large organization, if in your security architecture, you don't already have a DDoS protection service or tool, you need to build it into your roadmap in the future.

Brian Contos:

Yeah, I think that's sage advice, especially for the small and medium sized organizations that you mentioned that, a lot of them have the exact same risk profile. They just don't have the budget or have resources to address said risks. So, they have to look into services to help augment that. They have to look into some way to help address those and certainly, your telecom provider can go a long way to help in that. And then the bigger folks can start accessing some of their own enterprise tools that you mentioned.

Brian Contos:

And I think that's just great advice, and we're seeing that across the board even, we're even seeing large enterprises now starting to build... As I'm sure you're seeing... Our relationships with telecoms for that additional layer of support, right? That next tier, especially when it comes to DDoS because you don't have all the capabilities of mitigating DDoS might not just be on your network, you might have to take it a step higher, which of course is your telecom and various telecoms and their relationships.

Brian Contos:

I think that's some sage advice. What is funny, when you mentioned charging, you know, character generation. I was thinking back to the late 1990s, and there was a DoS attack, not even a DDoS attack, where you could Telnet into the character generation port, and it just generates zero through nine then eight through Z and then you redirect it to the echo port, which basically echoes at whatever you pipe in. So, if you pipe one to the other, you get in this continuous loop and you can actually bring the system down. And—

Mary Haynes:

Mm-hmm.

Brian Contos:

I had forgotten all about that for like the last 20 years until you brought it up. It's amazing that the old and the new are kind of all squished in there together. And there's still those... Those old school vulnerabilities are still out there. I just find that really amazing. A little bit amusing, but more amazing.

Mary Haynes:

Yeah! We actually used to use that to help educate our executives of how DDoS worked. It was a great way to demonstrate the threat that we were facing back in the 90s and again, still a threat today.

Brian Contos:

Yeah. Wow. Well I know beyond DDoS, there's one other thing that you're really passionate about and that relates to the diversity in the cybersecurity workplace and maybe you can give us a little bit of insight on that as well.

Mary Haynes:

You know, I didn't really realize what a challenge we had in our industry really until the last six or seven years. Sometimes when I tell people that, they're kind of surprised because like I said, I remember when I first joined into a security role, didn't think anything about, that I was the only girl on the team, didn't even ask questions about it. And I remember going to my first conference meeting with kind of an all hands meeting with my new peers, like about a month into my job, and walking into the conference room and realizing, "Yeah, I was the one in 30 at this conference." However, as organizations have been building out cybersecurity teams, and as I've started going to conferences, et cetera. It really became when I realized, "Gosh, I'm one of the few women here."

Mary Haynes:

I even got to a point about the mid 2000s, I kind of stopped going to security conferences because I felt so out of place. But the other part that I realized, it wasn't just a female issue, but also when I looked across the room, I saw a real lack of diversity in general. And I know just personally, the last few years, I've really been focusing on not how can we get more women in security? But also how can we get a more diverse profile. And I really do encourage the leaders that I have working for me every time they're looking at a candidate, asking the questions. Are there any diverse candidates out there? whether they're female or they've got different colors of skin, but we really need to build diversity.

Mary Haynes:

I've always had diverse teams prior to getting into security and I always realized it was so great to have the diverse thought, et cetera. And I think one of the biggest challenges we have in our industry, and why we haven't been able to win this fight, is we kind of want people that think alike. They look alike, they think alike, and we really need to get much more diverse thought on how to battle some of the challenges we face today. And that begins with a focus on diversity. I think we've got a real great opportunity as people talk about the challenges we have, and all of the jobs that are going to be available in the future in this particular profession. We have a tremendous opportunity to target some of our inner-city schools and where we have more diverse communities in our country. And really try to build cybersecurity interest, hopefully early on in their lifetime.

Mary Haynes:

I'm seeing a lot of friends in this industry who are really giving a lot on trying to work with some of the school districts. Not only trying to get into the high school age, but also get into the middle schools where we can try to convince people that, "Hey, this is a great career. You can go down this path and not get a college degree. And maybe follow in the steps in your community, which probably is not a good path to go. Or maybe you could go down this path, where you maybe even don't need a formal education if you get into technology right now in your young age, and really embrace this. And you can have a very, very profitable career." And I think it's going to be one of our keys to solving the challenges we have in staffing and cybersecurity. Not only today, but in the future.

Mary Haynes:

Only 54% of our kids today in the US go on to college. A lot of that's contributed to our inner-city schools where they don't see that as an opportunity for them, or even in our rural communities where they don't see a lot of people going on and getting that additional education. And we've got a tremendous opportunity to influence those communities into what could be really great career decisions for them in the future.

Mary Haynes:

So that's really my passion. I'm actually working on some interesting cybersecurity history research right now, that hopefully I'll be able to share and show how there's been tons of women in this field in the past that people didn't really realize it and recognize it. And there's actually been a lot of diverse contributors to this industry. So that maybe people can see others like themselves in this business so that we can really face that staffing challenge in the future.

Brian Contos:

Yeah, I love that. I'm always personally a big fan of sharing the history too. And you've got people like Ada Lovelace of course, and Grace Hopper and some of the others. I just named two of many. But there's been so many fantastic contributions. One of the things I always think is great about cybersecurity, as you talk to 10 cybersecurity professionals, and they always have such a diverse background about how they entered the field. Sure, some of them came up and they did the more traditional computer science or programming type background is how they got in. But a lot of them came over from sociology or economics backgrounds or no college at all and just kind of came in from different routes.

Brian Contos:

So I love that about it and I think that's helped quite a bit. And what you're saying is let's make it even more diverse. And I think that's definitely something that's needed and would certainly help. When you look at the same problem, upside down and backwards for long enough, it begins to look right. So if you get some more perspectives in there, it can only help things, right? In terms of, "Hey, why don't we think about this problem a little bit differently." So kudos to you for all your work on that Mary. So as we wrap up, there's a question that I like to ask all of our guests and that's, Mary, who's your favorite superhero or supervillain and why?

Mary Haynes:

Well, it's Invisible Woman or also known as Sue Storm Richards. So, I actually identify with her and by the way, I'm a huge Marvel fan like many of you are. But there's a lot of commonalities between her character, and us women that are in security today. For those of you who aren't familiar with Marvel comics and who Invisible Woman is, she has the ability to manipulate this cosmic energy that can then cause her and distort her body where she becomes invisible and then she can do that to others.

Mary Haynes:

And I always come up, laugh when I think about her because I always think, "Gosh! I wish I could be a fly on the wall" And listen to some of the stories of where I've come in. And I've said, "Oh, you've got to do this, this, this, this, this to make your system secure." And I know sometimes in the past those male engineers looked at me like, I have no idea what I was talking about. And that's when I wished I could just have those powers that Sue had and become invisible and listen to see what they say. But the other kind of commonalities that she brings, she was a matriarch of the female superheroes. One of the very first ones. And she was a working mom, and she emulates a lot of the things that I represent as well, and many of the women in security represent as well too.

Mary Haynes:

Not only can make herself invisible, but she can use her powers to protect against invisible, or protect against... I'm getting my words mixed up. We look at all the threats that we face, and we always say security needs to be an enabler, right? And our security controls really need to be transparent to the business as well as the end user that we're hired to protect. And again, I think she represents that, and I want to be one of those invisible women that kind of solve these mysteries, and protects our environment the way she protects all of those countries she was protecting with her powers in many of those Marvel movies. So that's why she's my superhero. I'm going to continue to go to each new Marvel movie that comes out in the future because I just love her character.

Brian Contos:

That's awesome. I love it. I love it. I got to say, as everybody that listens to this podcast knows I'm a big comic book collector and superhero fan and all that. We haven't done the Fantastic Four a great justice in the last few movies. I'm hoping we get like a really, really good one because there are some great characters, and certainly hasn't lived up to the level of X-Men and the Avengers and similar movies. I think we're due for a really good Fantastic Four featuring Sue.

Brian Contos:

So, well. Thank you so much Mary, and thanks to our listeners for joining and be sure to check out other Cybersecurity Effectiveness Podcasts sponsored by Verodin.