Matt: A professional on dealing with attacks

My name's Matt, I'm a chaos specialist at Google.
They let us choose our own job titles to best describe what it is we do.
I spend a lot of my time planning for
how to take care of anything that might possibly be going wrong, and
when it does happen, putting a team in place to fix it as quickly as possible.
I had no intention of being in technology at all.
In high school, I was a lifeguard, first at public pools and then at a state beach.
Lifeguarding got me into really enjoying rescue.
So I got an EMT license, went through firefighter school. About halfway through
my college process, and well into when I was being a firefighter on a daily basis.
I was dealing with some burnout, some stress.
I needed a change in my life.
And a friend of mine who I'd been online gaming with since the early days
of online gaming, when it was all text based,
he said, I can tell you're burning out hard and you need a change.
My friends and I are going to San Francisco to start a startup.
Will you come with us?
And I said, you realize I am not a computer guy, right?
And he said, no, you're a computer guy, you just won't admit it.
The same thing that has drawn me into incident response in tech is what
originally drew me to medical response.
I really love being there for people on their worst day.
Being there when people really need you and
they don't know where else to turn to has always just fed this part of me, and
I'm lucky to find that same joy in DFIR, Digital Forensics and Incident Response.
What type of attacks have we faced at Google?
That's a hard question to answer,
because we face all of the kinds of attacks that most other companies face.
People after ransomware, people after industrial secrets,
other countries looking for intelligence information.
There was a really interesting attack that occurred a little while ago.
They were interested in getting a lot of information from technical companies,
specifically about vulnerabilities in software.
And they put in place a long running campaign to build personalities on
social media as though they were legitimate security researchers, and
then reach out to other security researchers in our field,
build relationships, and then just at the right moment, sneak in some malware.
Being under attack by an adversary who's made some progress is incredibly
stressful.

The first things you're thinking and
feeling are a little bit of a sense of panic.
Oh no, this is going to be a bad day.
How long am I going to be awake working on this?
What have they done?
What am I going to do?
And for me, the mantra that I repeat to myself is, as an incident responder,
I am here to help.
The things that are most important to having a good outcome
in an incident are what we call the 3Cs: Command, Control and
Communications. Meaning someone needs to be in charge of it affirmatively leading.
Someone needs to be exerting control over everyone involved so
that everyone's aligned, focused on the mission, and the biggest and
most important one of them all: proper communications.
If you have something to offer to the incident,
don't just go do it, Communicate to someone.
I think I could do this to help us make progress.
I think if we look over here, we'll find more data.
The advice that I would give somebody who wants to get into cybersecurity is if you
want it, you probably belong here.
The more people we have in here, who are passionate, curious question askers,
who want to know more, who want to build better, and who care about
making every thing more secure for the people who have to use technology,
those are people we want in the industry and I would want you here.

Revision #1
Created 2023-07-01 06:34:09 UTC by naruzkurai
Updated 2023-07-03 10:29:21 UTC by naruzkurai