00:04

I want you to travel back in time with me, to the before time, to 2017. I don't know if you can remember it, dinosaurs were roaming the earth. I was a security researcher, I had spent about five or six years doing research on the ways in which APTs, which is short for advanced persistent threats, which stands for nation-state actors, spy on journalists and activists and lawyers and scientists and just generally people who speak truth to power.

00:42

And I'd been doing this for a while when I discovered that one of my fellow researchers, with whom I had been doing this all this time, was allegedly a serial rapist. So the first thing that I did was I read a bunch of articles about this. And in January of 2018, I read an article with some of his alleged victims. And one of the things that really struck me about this article is how scared they were. They were really frightened, they had, you know, tape over the cameras on their phones and on their laptops, and what they were worried about was that he was a hacker and he was going to hack into their stuff and he was going to ruin their lives. And this had kept them silent for a really long time.

01:36

So, I was furious. And I didn't want anyone to ever feel that way again. So I did what I usually do when I'm angry: I tweeted.

01:48

(Laughter)

01:50

And the thing that I tweeted was that if you are a woman who has been sexually abused by a hacker and that hacker has threatened to break into your devices, that you could contact me and I would try to make sure that your device got a full, sort of, forensic look over. And then I went to lunch.

02:10

(Laughter)

02:13

Ten thousand retweets later,

02:15

(Laughter)

02:16

I had accidentally started a project.

02:21

So every morning, I woke up and my mailbox was full. It was full of the stories of men and women telling me the worst thing that had ever happened to them. I was contacted by women who were being spied on by men, by men who were being spied on by men, by women who were being spied on by women, but the vast majority of the people contacting me were women who had been sexually abused by men who were now spying on them. The one particularly interesting case involved a man who came to me, because his boyfriend had outed him as gay to his extremely conservative Korean family. So this is not just men-spying-on-women issue.

03:13

And I'm here to share what I learned from this experience. What I learned is that data leaks. It's like water. It gets in places you don't want it. Human leaks. Your friends give away information about you. Your family gives away information about you. You go to a party, somebody tags you as having been there. And this is one of the ways in which abusers pick up information about you that you don't otherwise want them to know. It is not uncommon for abusers to go to friends and family and ask for information about their victims under the guise of being concerned about their "mental health."

03:56

A form of leak that I saw was actually what we call account compromise. So your Gmail account, your Twitter account, your Instagram account, your iCloud, your Apple ID, your Netflix, your TikTok -- I had to figure out what a TikTok was. If it had a login, I saw it compromised.

04:24

And the reason for that is because your abuser is not always your abuser. It is really common for people in relationships to share passwords. Furthermore, people who are intimate, who know a lot about each other, can guess each other's security questions. Or they can look over each other's shoulders to see what code they're using in order to lock their phones. They frequently have physical access to the phone, or they have physical access to the laptop. And this gives them a lot of opportunity to do things to people's accounts, which is very dangerous.

04:59

The good news is that we have advice for people to lock down their accounts. This advice already exists, and it comes down to this: Use strong, unique passwords for all of your accounts. Use more strong, unique passwords as the answers to your security questions, so that somebody who knows the name of your childhood pet can't reset your password. And finally, turn on the highest level of two-factor authentication that you're comfortable using. So that even if an abuser manages to steal your password, because they don't have the second factor, they will not be able to log into your account.

05:43

The other thing that you should do is you should take a look at the security and privacy tabs for most of your accounts. Most accounts have a security or privacy tab that tells you what devices are logging in, and it tells you where they're logging in from. For example, here I am, logging in to Facebook from the La Quinta, where we are having this meeting, and if for example, I took a look at my Facebook logins and I saw somebody logging in from Dubai, I would find that suspicious, because I have not been to Dubai in some time.

06:19

But sometimes, it really is a RAT. If by RAT you mean remote access tool. And remote access tool is essentially what we mean when we say stalkerware. So one of the reasons why getting full access to your device is really tempting for governments is the same reason why getting full access to your device is tempting for abusive partners and former partners.

06:48

We carry tracking devices around in our pockets all day long. We carry devices that contain all of our passwords, all of our communications, including our end-to-end encrypted communications. All of our emails, all of our contacts, all of our selfies are all in one place, often our financial information is also in this place. And so, full access to a person’s phone is the next best thing to full access to a person's mind.

07:19

And what stalkerware does is it gives you this access. So, you may ask, how does it work? The way stalkerware works is that it's a commercially available program, which an abuser purchases, installs on the device that they want to spy on, usually because they have physical access or they can trick their target into installing it themselves, by saying, you know, "This is a very important program you should install on your device." And then they pay the stalkerware company for access to a portal, which gives them all of the information from that device. And you're usually paying something like 40 bucks a month. So this kind of spying is remarkably cheap.

08:13

Do these companies know that their tools are being used as tools of abuse? Absolutely. If you take a look at the marketing copy for Cocospy, which is one of these products, it says right there on the website that Cocospy allows you to spy on your wife with ease, "You do not have to worry about where she goes, who she talks to or what websites she visits." So that's creepy.

08:42

HelloSpy, which is another such product, had a marketing page in which they spent most of their copy talking about the prevalence of cheating and how important it is to catch your partner cheating, including this fine picture of a man who has clearly just caught his partner cheating and has beaten her. She has a black eye, there is blood on her face. And I don't think that there is really a lot of question about whose side HelloSpy is on in this particular case. And who they're trying to sell their product to.

09:18

It turns out that if you have stalkerware on your computer or on your phone, it can be really difficult to know whether or not it's there. And one of the reasons for that is because antivirus companies often don't recognize stalkerware as malicious. They don't recognize it as a Trojan or as any of the other stuff that you would normally find that they would warn you about. These are some results from earlier this year from VirusTotal. I think that for one sample that I looked at I had something like a result of seven out of 60 of the platforms recognized the stalkerware that I was testing. And here is another one where I managed to get 10, 10 out of 61. So this is still some very bad results.

10:11

I have managed to convince a couple of antivirus companies to start marking stalkerware as malicious. So that all you have to do if you're worried about having this stuff on your computer is you download the program, you run a scan and it tells you "Hey, there's some potentially unwanted program on your device." It gives you the option of removing it, but it does not remove it automatically. And one of the reasons for that is because of the way that abuse works. Frequently, victims of abuse aren't sure whether or not they want to tip off their abuser by cutting off their access. Or they're worried that their abuser is going to escalate to violence or perhaps even greater violence than they've already been engaging in.

10:59

Kaspersky was one of the very first companies that said that they were going to start taking this seriously. And in November of this year, they issued a report in which they said that since they started tracking stalkerware among their users that they had seen an increase of 35 percent. Likewise, Lookout came out with a statement saying that they were going to take this much more seriously. And finally, a company called Malwarebytes also put out such a statement and said that they had found 2,500 programs in the time that they had been looking, which could be classified as stalkerware.

11:42

Finally, in November I helped to launch a coalition called the Coalition Against Stalkerware, made up of academics, people who are doing this sort of thing on the ground -- the practitioners of helping people to escape from intimate partner violence -- and antivirus companies. And our goal is both to educate people about these programs, but also to convince the antivirus companies to change the norm in how they act around this very scary software, so that soon, if I get up in front of you and I talk to you about this next year, I could tell you that the problem has been solved, and all you have to do is download any antivirus and it is considered normal for it to detect stalkerware. That is my hope.

12:40

Thank you very much.

12:41

(Applause)