Ted Talks: Everyday cybercrime – and what you can do about it

I'm going to be showing some of the cybercriminals' latest and nastiest creations. So basically, please don't go and download any of the viruses that I show you.

Some of you might be wondering what a cybersecurity specialist looks like, and I thought I'd give you a quick insight into my career so far. It's a pretty accurate description. This is what someone that specializes in malware and hacking looks like.

So today, computer viruses and trojans, designed to do everything from stealing data to watching you in your webcam to the theft of billions of dollars. Some malicious code today goes as far as targeting power, utilities and infrastructure.

Let me give you a quick snapshot of what malicious code is capable of today. Right now, every second, eight new users are joining the Internet. Today, we will see 250,000 individual new computer viruses. We will see 30,000 new infected websites. And, just to kind of tear down a myth here, lots of people think that when you get infected with a computer virus, it's because you went to a porn site. Right? Well, actually, statistically speaking, if you only visit porn sites, you're safer. People normally write that down, by the way. (Laughter) Actually, about 80 percent of these are small business websites getting infected.

Today's cybercriminal, what do they look like? Well, many of you have the image, don't you, of the spotty teenager sitting in a basement, hacking away for notoriety. But actually today, cybercriminals are wonderfully professional and organized. In fact, they have product adverts. You can go online and buy a hacking service to knock your business competitor offline. Check out this one I found.

(Video) Man: So you're here for one reason, and that reason is because you need your business competitors, rivals, haters, or whatever the reason is, or who, they are to go down. Well you, my friend, you've came to the right place. If you want your business competitors to go down, well, they can. If you want your rivals to go offline, well, they will. Not only that, we are providing a short-term-to-long-term DDOS service or scheduled attack, starting five dollars per hour for small personal websites to 10 to 50 dollars per hour.

James Lyne: Now, I did actually pay one of these cybercriminals to attack my own website. Things got a bit tricky when I tried to expense it at the company. Turns out that's not cool. But regardless, it's amazing how many products and services are available now to cybercriminals. For example, this testing platform, which enables the cybercriminals to test the quality of their viruses before they release them on the world. For a small fee, they can upload it and make sure everything is good.

But it goes further. Cybercriminals now have crime packs with business intelligence reporting dashboards to manage the distribution of their malicious code. This is the market leader in malware distribution, the Black Hole Exploit Pack, responsible for nearly one third of malware distribution in the last couple of quarters. It comes with technical installation guides, video setup routines, and get this, technical support. You can email the cybercriminals and they'll tell you how to set up your illegal hacking server.

So let me show you what malicious code looks like today. What I've got here is two systems, an attacker, which I've made look all Matrix-y and scary, and a victim, which you might recognize from home or work. Now normally, these would be on different sides of the planet or of the Internet, but I've put them side by side because it makes things much more interesting.

Now, there are many ways you can get infected. You will have come in contact with some of them. Maybe some of you have received an email that says something like, "Hi, I'm a Nigerian banker, and I'd like to give you 53 billion dollars because I like your face." Or funnycats.exe, which rumor has it was quite successful in China's recent campaign against America.

Now there are many ways you can get infected. I want to show you a couple of my favorites. This is a little USB key. Now how do you get a USB key to run in a

business? Well, you could try looking really cute. Awww. Or, in my case, awkward and pathetic. So imagine this scenario: I walk into one of your businesses, looking very awkward and pathetic, with a copy of my C.V. which I've covered in coffee, and I ask the receptionist to plug in this USB key and print me a new one. So let's have a look here on my victim computer. What I'm going to do is plug in the USB key. After a couple of seconds, things start to happen on the computer on their own, usually a bad sign. This would, of course, normally happen in a couple of seconds, really, really quickly, but I've kind of slowed it down so you can actually see the attack occurring. Malware is very boring otherwise. So this is writing out the malicious code, and a few seconds later, on the left-hand side, you'll see the attacker's screen get some interesting new text. Now if I place the mouse cursor over it, this is what we call a command prompt, and using this we can navigate around the computer. We can access your documents, your data. You can turn on the webcam. That can be very embarrassing. Or just to really prove a point, we can launch programs like my personal favorite, the Windows Calculator.

So isn't it amazing how much control the attackers can get with such a simple operation? Let me show you how most malware is now distributed today. What I'm going to do is open up a website that I wrote. It's a terrible website. It's got really awful graphics. And it's got a

comments section here where we can submit comments to the website. Many of you will have used something a bit like this before. Unfortunately, when this was implemented, the developer was slightly inebriated and managed to forget all of the secure coding practices he had learned. So let's imagine that our attacker, called Evil Hacker just for comedy value, inserts something a little nasty. This is a script. It's code which will be interpreted on the webpage. So I'm going to submit this post, and then, on my victim computer, I'm going to open up the web browser and browse to my website, www.incrediblyhacked.com. Notice that after a couple of seconds, I get redirected. That website address at the top there, which you can just about see, microshaft.com, the browser crashes as it hits one of these exploit packs, and up pops fake antivirus. This is a virus pretending to look like antivirus software, and it will go through and it will scan the system, have a look at what its popping up here. It creates some very serious alerts. Oh look, a child porn proxy server. We really should clean that up. What's really insulting about this is not only does it provide the attackers with access to your data, but when the scan finishes, they tell you in order to clean up the fake viruses, you have to register the product. Now I liked it better when viruses were free. (Laughter) People now pay cybercriminals money to run viruses, which I find utterly bizarre.

So anyway, let me change pace a little bit. Chasing 250,000 pieces of malware a day is a massive challenge, and those numbers are only growing directly in proportion to the length of my stress line, you'll note here. So I want to talk to you briefly about a group of hackers we tracked for a year and actually found -- and this is a rare treat in our job. Now this was a cross-industry collaboration, people from Facebook, independent researchers, guys from Sophos. So here we have a couple of documents which our cybercriminals had uploaded to a cloud service, kind of like Dropbox or SkyDrive, like many of you might use. At the top, you'll notice a section of source code. What this would do is send the cybercriminals a text message every day telling them how much money they'd made that day, so a kind of cybercriminal billings report, if you will. If you look closely, you'll notice a series of what are Russian telephone numbers. Now that's obviously interesting, because that gives us a way of finding our cybercriminals. Down below, highlighted in red, in the other section of source code, is this bit "leded:leded." That's a username, kind of like you might have on Twitter.

So let's take this a little further. There are a few other interesting pieces the cybercriminals had uploaded. Lots of you here will use smartphones to take photos and post them from the conference. An interesting feature of lots of modern smartphones is that when you take a photo, it embeds GPS data about where that photo was taken. In fact, I've been spending a lot of time on Internet dating sites recently, obviously for research purposes, and I've noticed that about 60 percent of the profile pictures on Internet dating sites contain the GPS coordinates of where the photo was taken, which is kind of scary because you wouldn't give out your home address to lots of strangers, but we're happy to give away our GPS coordinates to plus or minus 15 meters. And our cybercriminals had done the same thing. So here's a photo which resolves to St. Petersburg. We then deploy the incredibly advanced hacking tool. We used Google. Using the email address, the telephone number and the GPS data, on the left you see an advert for a BMW that one of our cybercriminals is selling, on the other side an advert for the sale of sphynx kittens. One of these was more stereotypical for me. A little more searching, and here's our cybercriminal. Imagine, these are hardened cybercriminals sharing information scarcely. Imagine what you could find about each of the people in this room. A bit more searching through the profile and there's a photo of their office. They were working on the third floor. And you can also see some photos from his business companion where he has a taste in a certain kind of image. It turns out he's a member of the Russian Adult Webmasters Federation.

But this is where our investigation starts to slow down. The cybercriminals have locked down their profiles quite well. And herein is the greatest lesson of social media and mobile devices for all of us right now. Our friends, our families and our colleagues can break our security even when we do the right things. This is MobSoft, one of the companies that this cybercriminal gang owned, and an interesting thing about MobSoft is the 50-percent owner of this posted a job advert, and this job advert matched one of the telephone numbers from the code earlier. This woman was Maria, and Maria is the wife of one of our cybercriminals. And it's kind of like she went into her social media settings and clicked on every option imaginable to make herself really, really insecure. By the end of the investigation, where you can read the full 27-page report at that link, we had photos of the cybercriminals, even the office Christmas party when they were out on an outing. That's right, cybercriminals do have Christmas parties, as it turns out. Now you're probably wondering what happened to these guys. Let me come back to that in just a minute.

I want to change pace to one last little demonstration, a technique that is wonderfully simple and basic, but is interesting in exposing how much information we're all giving away, and it's relevant because it applies to us as a TED audience. This is normally when people start kind of shuffling in their pockets trying to turn their phones onto airplane mode desperately.

Many of you all know about the concept of scanning for wireless networks. You do it every time you take out your iPhone or your Blackberry and connect to something like TEDAttendees. But what you might not know is that you're also beaming out a list of networks you've previously connected to, even when you're not using wireless actively. So I ran a little scan. I was relatively inhibited compared to the cybercriminals, who wouldn't be so concerned by law, and here you can see my mobile device. Okay? So you can see a list of wireless networks. TEDAttendees, HyattLB. Where do you think I'm staying? My home network, PrettyFlyForAWifi, which I think is a great name. Sophos_Visitors, SANSEMEA, companies I work with. Loganwifi, that's in Boston. HiltonLondon. CIASurveillanceVan. We called it that at one of our conferences because we thought that would freak people out, which is quite fun. This is how geeks party.

So let's make this a little bit more interesting. Let's talk about you. Twenty-three percent of you have been to Starbucks recently and used the wireless network. Things get more interesting. Forty-six percent of you I could link to a business, XYZ Employee network. This isn't an exact science, but it gets pretty accurate. Seven hundred and sixty-one of you I could identify a hotel you'd been to recently, absolutely with pinpoint precision somewhere on the globe. Two hundred and thirty-four of you, well, I know where you live. Your wireless network name is so unique that I was able to pinpoint it using data available openly on the Internet with no hacking or clever, clever tricks. And I should mention as well that some of you do use your names, "James Lyne's iPhone," for example. And two percent of you have a tendency to extreme profanity.

So something for you to think about: As we adopt these new applications and mobile devices, as we play with these shiny new toys, how much are we trading off convenience for privacy and security? Next time you install something, look at the settings and ask yourself, "Is this information that I want to share? Would someone be able to abuse it?"

We also need to think very carefully about how we develop our future talent pool. You see, technology's changing at a staggering rate, and that 250,000 pieces of malware won't stay the same for long. There's a very concerning trend that whilst many people coming out of schools now are much more technology-savvy, they know how to use technology, fewer and fewer people are following the feeder subjects to know how that technology works under the covers. In the U.K., a 60 percent reduction since 2003, and there are similar statistics all over the world.

We also need to think about the legal issues in this area. The cybercriminals I talked about, despite theft of millions of dollars, actually still haven't been arrested, and at this point possibly never will. Most laws are national in their implementation, despite cybercrime conventions, where the Internet is borderless and international by definition. Countries do not agree, which makes this area exceptionally challenging from a legal perspective.

But my biggest ask is this: You see, you're going to leave here and you're going to see some astonishing stories in the news. You're going to read about malware doing incredible and terrifying, scary things. However, 99 percent of it works because people fail to do the basics. So my ask is this: Go online, find these simple best practices, find out how to update and patch your computer. Get a secure password. Make sure you use a different password on each of your sites and services online. Find these resources. Apply them.

The Internet is a fantastic resource for business, for political expression, for art and for learning. Help me and the security community make life much, much more difficult for cybercriminals.

Thank you.

(Applause)