**Ransomware on demand?**

Carl: Alright Mike, so what are you going to show us today?

Mike: So recently we saw the WannaCry ransom attack and we’re going to show some similar ransom attacks from both sides. We’re going to show you the hackers from the control centre and the victim’s machine, and how it looks from each.

Carl: And what are you hoping to show people through doing this?

Mike: I want to show people how easy it is to set up and how easy it is for a hacker to control.This is not labour intensive at all. You could quite happily encrypt 10,000 of these and not be tired, whatsoever. How easily it is to protect yourself from it, is another key point. Really we will show three angles of it.

Carl: And is it possible for people to protect themselves, it feels like cyberattacks are becoming more and more frequent, and more and more serious?

Mike: That’s true. Is there a way to protect yourself entirely? In reality, no, probably not. But that doesn’t mean you can’t use the internet. I think we’ve just got to be realistic on what our vulnerabilities are and how we can try to stop ourselves from being exploited through those vulnerabilities by understanding the realities of what we face.

I think this will be an eye-opener for people. When they see this, and how it works, and how easy it is, they will start to think, actually this isn’t a highly complicated attack. This isn’t something only ten people in the world can do.

Carl: Hopefully we won’t inspire anyone to go out and do attacks themselves.

Mike: Exactly. No, hopefully not. But also the main thing is the motive. Who out there really wants to carry out these attacks? No many people. When the WannaCry attack happened I saw a huge backlash from the hacker community where a lot of people who ordinarily use botnets for criminal activity turned out onto this phorest to try and stop it. Most of them didn’t succeed,, but they still tried because the reality is, many of the people in our community don’t want to see this type of attack. It was too dangerous.

Carl: And they don’t want to see hospitals being brought down…?

Mike: That’s no-one’s intention. I think there’s probably a select few people in the world who would actively target hospitals. Otherwise we would see it every day. The reality of it is that companies are targeted every day, not hospitals, and that’s for a reason…

Carl: So, what do we know about WannaCry so far?

Mike: It was a relatively old piece of kit. WannaCry was origianally called WannaCryptor, which was shortened to WannaCry in the wake of the recent attack. It is a very strong piece of malware. The issue with a lot of these pieces of malware is that they basically stay one step ahead of anti-virus companies. When someone makes a piece of software like WannaCry or Rainmaker labs - the piece of malware that we’re going to show the viewer today - they will put out a flawed version of the software which will make companies like McCarthy and Norton pop-up and say we can decrypt Rainmaker, when in reality, Rainmaker labs then release a much stronger version two and a half weeks later, that can’t be decrypted. So now you have a piece of ransomware which can’t be decrypted and a lot of anti-virus companies saying it can be. This is very, very dangerous. People are buying equipment thinking they are going to be protected from attacks and in reality they’re not. The software itself it is extremely well written by some highly capable people…

Carl: And do we know who was behind the attack?

Mike: We know who was behind the software. We know the NSA wrote the original exploit, which a lot of the people in our community don’t necessarily have an issue with, if you can keep them secure. GCHQ probably have similar sorts of software but they don’t seem to have the leaks the NSA have. But, were the makers of WannaCry behind it? No, they weren’t, they didn’t even know it was going to be used for this. They just wrote some ransomware and said to users, use it for what you want. If they knew this was going to happen, they probably wouldn’t have released it….

Carl: So, for anyone that sees this and is afraid about how easy it is to conduct malware attacks, what are the three things that you need to remember to keep safe, or at least ‘safer’, online?

Mike: The main thing is real-time backups. It doesn’t matter how you are attacked if you backup. You can be attacked in anyway at all; with a cryptor attack, destruction attack or other attacks. If you’ve got backups it’s fine. You’ll re-install it, that’s it.