Bsides Cymru/Cardiff

On Saturday 11th February 2023 I attended the Bsides Cymru/Cardiff conference. Conferences are a good place to build connections, expand your knowledge in your field and learn new things. This one is an Infosec community gathering that provides a place to connect and share knowledge. Here's a rundown of the presentations I managed to see. With 3 tracks and 3 workshops it's not possible to do it all but here's a rundown of the presentations I managed to attend.

First up was The Keynote/Opening speech which was given by John Shier, a Senior Research Scientist at Sophos. John talked to us about 'What cyber criminals can teach us', in particular adaptation and evolution. An example given was the use of ChatGPT to write scam emails. This eliminated some of the fake email tell-tale signs that people are trained to look out for such as spelling and grammar mistakes and created quite a convincing email. If the cyber criminals are adapting their techniques with any new tools available then we as defenders also need to adapt and evolve to combat them. It's something we've always had to do but now the access to the tools to commit cyber crime are more easily obtainable than ever before.

The next session I went to was 'Robots for Complete Beginners' by Mark Goodwin. The talk started with mention of 'Chuckie Egg' which for those born in the years after the ZX Spectrum era is an old home computer video game based on collecting eggs. This was clearly the beginning of his love of chickens as the talk moved on to how he has used robots for egg incubation, chicken monitoring and closing the gates after the chickens go home. With these real world usages for robots in mind the presentation moved on to the basics of building robots from scratch, what materials are needed, how to create the code and also several demonstrations of the robots in action. I'm not sure what sacrifices were made to the Demo Gods before the talk but they were definitely sated and all the demos were successful. At the end Mark demonstrated how accessible the parts can be as the robots can be made out of Lego Technic.

Next up was ‘Giving you the ICK - Industrial Cyber Knowledge for n00bs’ by Jamie Grant. This was a scary look at what damage can be caused when Industrial Systems are sabotaged. Jamie explained the ways to protect from this happening through regulations, reasonable security measures and effective training.

Onto something different again with ‘Trust & Blame in Self-Driving Cars Following a Cyber Attack’ by Victoria Marcinkiewicz. The question was asked if people trust self-driving cars and how much does that trust diminish after a road traffic accident and does the way the information is presented affect that trust. Is there less trust when there’s a possibility of a cyber attack involved. There was an interesting clip of police officers trying to pull over a car for having no headlights on only to find there was no driver which raises interesting questions on how that kind of situation should be dealt with.

The next talk I attended was ‘Bohemian IcedID - Queen of Loaders’ by Josh Hopkins and Thibault Seret. This was about threat research and the tracking of IcedID which started as a banking trojan and is now a standard malware dropper. The malware uses BackConnect to maintain persistence and the talk went into many of the details discovered through their research on the malware.

The next presentation was an interactive talk ‘The Office of Danger: A Choose Your Own adventure story!’ by Phil Eveleigh. It starts with the scope of your assignment for a 2 day physical security risk assessment. The audience are all given a card that is blue on one side yellow on the other. Throughout the story the audience are asked which of two options they want to take. At the end of the day in the story the path taken was compared to a real life assessment. This was a fantastic talk that explained the challenges of this type of assessment and kept the audience engaged and involved. The presenter has created a website of the talk so you can play along for yourself. Have a go here : https://blog.yekki.co.uk/Office/Danger.html

The next presentation I saw was ‘Hacking to defend: How we hacked into a Polar Orbit Satellite and managed to get a full system compromise’ by James (0xJay) and Josh Allman. These two researchers explained how they came across information on a Discord channel about how to gain unauthenticated access to a satellite. Discord is an instant messaging social platform. On investigating they found that this had not been rebooted in 14 years. The talk took us through the difficulties in finding right contacts to disclose the information to.

Finally I saw one last presentation which was ‘it's borked - programming was a mistake’ by Maya. This was a journey through different coding languages and trials and tribulations with the various different languages. From Python to PHP to java and beyond the various problems with each one was laid bare.

In-between the talks there were people to talk to, vendor stalls to peruse and BattleBots to watch. All in all a thoroughly enjoyable day.