Blackhat and DEFCON 2017 highlights

as written by Jacky Fox

The annual blackhat and DEFCON security conferences took place last week in the US. This is a gathering of cyber security professionals, hackers and incident responders where leading edge research and though leadership is presented to the community. Jacky Fox, Deloitte's Cyber Security and IT Forensic lead, provides some highlights from the conference below.

Refocusing the security community on defence and making security work for everyone - Alex Stamos

An inspiring keynote outlining how the security industry as a whole is not keeping pace with the threats we face. Alex suggested that we change our thinking from the 'stupid user' clicked the link to asking ourselves why we did not protect the user from the threat. He further detailed that we need to be more inclusive in security and attract and retain more women into the industry. A topic close to my heart, with women representing only 10% of cyber security professionals. Think of all the talent we are missing out on and the impact it would have on the 'good guys' team if we could change this.

Industroyer/Crashoverride, power grid targeting - Robert Lee, Joe Slowik, Ben Miller, Robert Lipovsky, Anton Cherepanov

To date there are four known types of energy related industrial control system malware, Stuxnet, Havex, BlackEnergy2 and Crashoverride. The latter was used to target the Ukraine in 2016 causing power outages. This malware is currently designed to target EU grids but it's modular design means that it can be tailored to hit the US. Some elements of this malware are used for network discovery but the main focus is to take over the control of power distribution substations, remove monitoring and visibility of the network and ultimately wipe the the HMI systems that would be needed to regain control of the network. Each instance of this type of attack needs a lot of reconnaissance and customisation. It cannot spread like a wannacry and needs considerable time and effort to be deployed.

ShieldFS a ransomware resilient file system - Andrea Continella, Frederico Maggi

This concept was incredibly simple and incredibly smart, with some clever coding in the background. Basically a virtual file system is setup that makes an on the fly backup of all files prior to a write instruction. It also incorporates the ability to detect large encryption operations and flag or halt the write operations. Finally there is a rollback feature to revert to the original files in the event of an unauthorised crypto event. While it is early days I suspect we will see the concept in reality soon.

Insecurity in building automation - Thomas Brandstetter

Building automation is typically used today for heating, ventilation, climate control and lighting. It is often seen as a poor relation when it comes to the pecking order for prioritisation for penetration testing. However, think of the impact on the ability to conduct your business if you make a building uninhabitable. There are many tools available that facilitate the scanning and enumeration of building automation devices, many of which are internet facing. We need to pay attention to this.

Go to hunt and then sleep - David Bianco, Robert Lee

Presentation of a practical and mathematical model to identify and prioritise the treatment of organisation specific threats. While it seems like common sense I suspect steps sometimes get missed here resulting in incomplete threat data and suboptimal treatment plans. Basically you need to Identify your assets and potential threats and then gather data on the threat lifecycle and the potential impact of the threats if realised. You can then make a plan by plotting techniques and tactics to enable better avoidance, identification and treatment. The use of automation here is highly recommended.

Attacking encrypted USB Keys the hard way - Jean-Michelle Picod, Elie Bursztein

This investigation proposed a methodology for auditing the security of encrypted USB sticks. A USB stick is made up of several components and variables; the input connector, the controller, storage, cryptography standard and the manufacturer. Some practical attacks and surprising vulnerabilities were demonstrated showing that not all manufacturers and devices are adhering to proper implementation of FIPS-140. The presenters requested that a better audit and certification process be put in place.

The brain's last stand - Garry Kasparov

The chess master who battled, won and lost against early artificial intelligence chess master simulators shared his wisdom on the human being vs AI. He concludes that the AI revolution will change our lives but the importance and role of the human will not diminish it will just change. A particularly good quote from Pablo Picasso 'Computers are useless, they can only give you answers'. Bring it on.

Hacking democracy a Socratic dialogue - Sean Kanuk

This interactive discussion raised multiple questions on how an election could be impacted by various hacking techniques from; opinion 'influencing' by indirect means, manipulation of vote

tallying machines, the integrity of the electoral register, influencing population movement, to name a few. The on site voting machine hacking village gave further weight to these concerns with multiple vulnerabilities discovered.

Contact: Jacky Fox

Recommendations:

https://www2.deloitte.com/ie/en/pages/risk/articles/new-perspectives-on-cyber-risk.html

https://www2.deloitte.com/ie/en/pages/risk/articles/assessing-cyber-risk.html