1400 - See no evil, hear no evil: Hacking invisibly and silently with light and sound

Thursday at 14:00 in 101 Track 2
45 minutes | Demo, Tool
Matt Wixey*Senior Associate, PwC*

Traditional techniques for C2 channels, exfiltration, surveillance, and exploitation are often frustrated by the growing sophistication and prevalence of security protections, monitoring solutions, and controls. Whilst all is definitely not lost, from an attacker's perspective - we constantly see examples of attackers creatively bypassing such protections - it is always beneficial to have more weapons in one's arsenal, particularly when coming up against heavily-defended networks and highly-secured environments.

This talk demonstrates a number of techniques and attacks which leverage light and/or sound, using off-the-shelf hardware. It covers everything from C2 channels and exfiltration using light and near-ultrasonic sound, to disabling and disrupting motion detectors; from laser microphones, to repelling drones; from trolling friends, to jamming speech and demotivating malware analysts.

This talk not only provides attendees with a new suite of techniques and methodologies to consider when coming up against a well-defended target, but also demonstrates, in a hopefully fun and practical way, how these techniques work, their advantages, disadvantages, and possible future developments. It also gives details of real case studies where some of these techniques have been used, and provides defenders with realistic methods for the mitigation of these attacks.

Finally, the talk covers some ideas for future research in this area.
Matt Wixey
Matt Wixey is a penetration tester on PwC's Threat and Vulnerability Management team in the UK, and leads the team's research function. Prior to joining PwC, he led a technical R&D team in a UK law enforcement agency. His research interests include bypassing air-gaps, antivirus and sandbox technologies, and RF hacking.

@darkartlab

#defcon25/by_track/101-Track2/Thursday #defcon25/By_Day/_thursday