1100 - From Box to Backdoor: Using Old School Tools and Techniques to Discover Backdoors in Modern Devices

Thursday at 11:00 in 101 Track
45 minutes
Patrick DeSantis*Senior Security Research Engineer, Cisco Talos*

Stringing together the exploitation of several seemingly uninteresting vulnerabilities can be a fun challenge for security researchers, penetration testers, and malicious attackers. This talk follows some of the paths and thought processes that one researcher followed while evaluating the security of several new "out of the box" Industrial Control System (ICS) and Internet of Things (IoT) devices, using a variety of well known exploitation and analysis techniques, and eventually finding undocumented, root-level, and sometimes un-removable, backdoor accounts.

Patrick DeSantis

Patrick DeSantis is a security researcher with Cisco Talos and focuses his efforts on discovery and exploitation of vulnerabilities in technologies that have an impact on the physical world, such as Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), Internet of Things (IoT), and anything else that looks like it's asking to be hacked. Patrick's background includes work in both the public and private sectors, as well as a pile of information security certifications and a few college degrees.

@pat_r10t

#defcon25/by_track/101/thursday #defcon25/By_Day/_thursday