1200 - The call is coming from inside the house! Are you ready for the next evolution in DDoS attacks?

Sunday at 12:00 in Track 3
45 minutes | Art of Defense

Steinthor Bjarnason*Senior Network Security Analyst, Arbor Networks*

Jason Jones*Security Architect, Arbor Networks*

The second half of 2016 saw the rise of a new generation of IoT botnets consisting of webcams and other IoT devices. These botnets were then subsequently used to launch DDoS attacks on an unprecedented scale against Olympic-affiliated organizations, OVH, the web site of Brian Krebs and Dyn.

Early 2017, a multi-stage Windows Trojan containing code to scan for vulnerable IoT devices and inject them with Mirai bot code was discovered. The number of IoT devices which were previously safely hidden inside corporate perimeters, vastly exceeds those directly accessible from the Internet, allowing for the creation of botnets with unprecedented reach and scale.

This reveals an evolution in the threat landscape that most organizations are completely unprepared to deal with and will require a fundamental shift in how we defend against DDoS attacks.

This presentation will include:

- An analysis of the Windows Mirai seeder including its design, history, infection vectors and potential evolution.
- The DDoS capabilities of typically infected IoT devices including malicious traffic analysis.
- The consequences of infected IoT devices inside the corporate network including the impact of DDoS attacks, originating from the inside, targeting corporate assets and external resources.
- How to detect, classify and mitigate this new threat.

Steinthor Bjarnason
Steinthor Bjarnason is a Senior Network Security Analyst on Arbor Networks ASERT team, performing applied research on new technologies and solutions to defend against DDoS attacks.

Steinthor has 17 years of experience working on Internet Security, Cloud Security, SDN Security, Core Network Security and DDoS attack mitigation. Steinthor is an inventor and principal of the Cisco Autonomic Networking Initiative, with a specific focus on Security Automation where he holds a number of related patents.

@sbjarnas
Jason Jones
Jason Jones is the Security Architect for Arbor Networks' ASERT team. His primary role involves reverse engineering malware, architecting of internal malware processing infrastructure, feed infrastructure and botnet monitoring infrastructure in addition to other development tasks. Jason has spoken at various industry conferences including BlackHat USA, FIRST, BotConf, REcon, and Ruxcon

#defcon25/by_track/track3/sunday #defcon25/By_Day/_Sunday