Security: Domain Name System, Department of Homeland Security, and Underclocking the ESP8266 Leads to WIFI Weirdness

By *Roy Schestowitz*
Created *12/01/2019 - 1:25am*
Submitted by Roy Schestowitz on Saturday 12th of January 2019 01:25:33 AM Filed under Security [1]

- **A DNS hijacking wave is targeting companies at an almost unprecedented scale [2]**

  The attacks, which security firm FireEye said have been active since January 2017, use three different ways to manipulate the Domain Name System records that allow computers to find a company's computers on the Internet. By replacing the legitimate IP address for a domain such as example.com with a booby-trapped address, attackers can cause example.com to carry out a variety of malicious activities, including harvesting user?s login credentials. The techniques detected by FireEye are particularly effective, because they allow attackers to obtain valid TLS certificates that prevent browsers from detecting the hijacking.

- **Worries mount as cybersecurity agency struggles amid shutdown [3]**

  Former Department of Homeland Security (DHS) officials and lawmakers fear the shutdown, now in its 20th day, could have both short- and long-term effects, hurting the new Cybersecurity and Infrastructure Security Agency?s (CISA) efforts to get off the ground and potentially pushing existing talent out the door.

- **Underclocking the ESP8266 Leads to WIFI Weirdness [4]**

Now it was time for another of those basic questions. What would happen if you did the same thing to a second ESP8266? Much to his surprise, [CNLohr] discovered that the two devices could still communicate successfully as long as their BBPLL clock speed was the same. From an outsider?s perspective it looked like gibberish, but to the two ESPs which had been slowed by the same amount, everything worked as expected even though the 802.11 standards say it shouldn?t.

So what can you do with this? The most obvious application is a ?stealth? WiFi connection between ESP8266s which wouldn?t show up to normal devices, a communications channel invisible to all but the most astute eavesdropper. [CNLohr] has made all the source code to pull this trick off public on GitHub, and it should be interesting to see what kind of applications (if any) hackers find for this standards-breaking behavior.

Security

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://arstechnica.com/information-technology/2019/01/a-dns-hijacking-wave-is-targeting-companies-at-an-almost-unprecedented-scale/
[3] https://thehill.com/policy/national-security/424649-worries-mount-as-cybersecurity-agency-struggles-amid-shutdown
[4] https://hackaday.com/2019/01/04/underclocking-the-esp8266-leads-to-wifi-weirdness/