1200 - DNS - Devious Name Services - Destroying Privacy & Anonymity Without Your Consent

Saturday at 12:00 in Track 3
45 minutes | Art of Defense
Jim Nitterauer*Senior Security Specialist, AppRiver, LLC*

You've planned this engagement for weeks. Everything's mapped out. You have tested all your proxy and VPN connections. You are confident your anonymity will be protected. You fire off the first round and begin attacking your target. Suddenly something goes south. Your access to the target site is completely blocked no matter what proxy or VPN you use. Soon, your ISP contacts you reminding you of their TOS while referencing complaints from the target of your engagement. You quickly switch MAC addresses and retry only to find that you are quickly blocked again!

What happened? How were you betrayed? The culprit? Your dastardly DNS resolvers and more specifically, the use of certain EDNS0 options by those resolvers.

This presentation will cover the ways in which EDNS OPT code data can divulge details about your online activity, look at methods for discovering implementation by upstream DNS providers and discuss ways in which malicious actors can abuse these features. We will also examine steps you can take to protect yourself from these invasive disclosures.

The details covered will be only moderately technical. Having a basic understanding of RFC 6891 and general DNS processes will help in understanding. We will discuss the use of basic tools including Wireshark, Packetbeat, Graylog and Dig.
Jim Nitterauer
Currently a Senior Security Specialist at AppRiver, LLC., his team is responsible for global network deployments and manages the SecureSurf global DNS infrastructure and SecureTide global spam & virus filtering infrastructure as well as all internal applications. They also manage security operations for the entire company. He holds a CISSP certification. He is also well-versed in ethical hacking and penetration testing techniques and has been involved in technology since the late 1980s when punch cards were still a thing.

Jim has presented at NolaCon, ITEN WIRED, BSides Las Vegas, BSides Atlanta, CircleCityCon and several smaller conferences. He regularly attends national security conferences and is passionate about conveying the importance of developing, implementing and maintaining security policies for organizations. His talks convey unique and practical techniques that help

attendees harden their security in practical and easy-to-deploy ways.

Jim is a senior staff member with BSides Las Vegas, a member of the ITEN WIRED Planning Committee and the president of the Florida Panhandle (ISC)2 Chapter. When not at the computer, Jim can be found working out, playing guitar, traveling or just relaxing with an adult beverage.

Twitter: @jnitterauer
LinkedIn: https://www.linkedin.com/in/jnitterauer/

#defcon25/by_track/track3/saturday #defcon25/By_Day/_saturday