1130 - Abusing Webhooks for Command and Control

Saturday at 11:30 in 101 Track
20 minutes | Demo, Tool
Dimitry Snezhkov*Security Consultant, X-Force Red, IBM*

You are on the inside of the perimeter. And maybe you want to exfiltrate data, download a tool, or execute commands on your command and control server (C2). Problem is - the first leg of connectivity to your C2 is denied. Your DNS and ICMP traffic is being monitored. Access to your cloud drives is restricted. You've implemented domain fronting for your C2 only to discover it is ranked low by the content proxy, which is only allowing access to a handful of business related websites on the outside.

We have all been there, seeing frustrating proxy denies or triggering security alarms making our presence known.
Having more choices when it comes to outbound network connectivity helps. In this talk we'll present a technique to establish such connectivity with the help of HTTP callbacks (webhooks). We will walk you through what webhooks are, how they are used by organizations. We will then discuss how you can use approved sites as brokers of your communication, perform data transfers, establish almost realtime asynchronous command execution, and even create a command-and-control communication over them, bypassing strict defensive proxies, and even avoiding attribution.

Finally, we'll release the tool that will use the concept of a broker website to work with the external C2 using webhooks.
Dimitry Snezhkov
Dimitry Snezhkov does not like to refer to himself in the third person ;) but when he does he is a Sr. Security Consultant for X-Force Red at IBM, currently focusing on offensive security testing, code hacking and tool building.

@Op_Nomad

#defcon25/by_track/101/saturday #defcon25/By_Day/_saturday