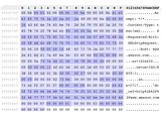
Justin Warner

76 followers

Follow

Home Activity New About

Using Kaitai to Parse Cobalt Strike Beacon Configs



I have seen a definite uptick in security researchers hunting Cobalt Strike servers, and tweeting/sharing indicators or config data. There...

Apr 6, 2021

Do You Miss Being a Red Teamer?

It is a question that gets posed to me pretty frequently: “Do you miss being a red teamer?” If you came all the way to my blog to see the...

Jul 23, 2018

Infrastructure Diversity—Hunting In Shared Infrastructure

As an attacker, it is all too easy to settle down into a rhythm. That rhythm of operations, the specific techniques and automation involved...

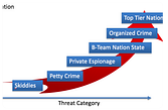
Apr 5, 2017

Common Ground Part 3: Execution and the People Factor

This is part t ne
background

Jul 5, 2016

Common Ground: Planning is Key



This is part two of a blog series titled: Common Ground. In , I discussed the backgrounds and evolution of red teaming, diving deep into...

Jun 28, 2016

Common Ground Part 1: Red Team History & Overview

Over the past ten years, red teaming has grown in popularity and has been adopted across different industries as a mature method of...

Jun 24, 2016

Creepy User-Centric Post-Exploitation

I love seeing red and blue teams square off during an engagement. It works best if both sides avoid selfish desires and focus on the task...

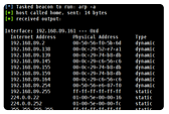
May 16, 2016

Empire & Tool Diversity: Integration is Key

Since the release of PowerShell Empire at BSidesLV 2015 by Will Schroeder (@harmj0y) and myself, the project has taken off. I could not be...

Feb 11, 2016

Remote W



Network attacks (WPAD injection, HTTP/WSUS MITM, SMB Relay etc.) are a very useful attack vector for adversaries trying to laterally...

Feb 5, 2016

Derivative Local Admin

Intro

Jun 5, 2015
