Tracking the Crypter and the Actor, viXra.org e-Print archive, viXra:1902.0257

Authors: Jason Reaves

In the world of malware crypters and packers are often time considered throwaway by researchers, it’s also fairly common to use them as training tools for junior personnel. In a way most obfuscations are treated as training, learning or for games like CTF(Capture The Flag). So it’s probably not surprising that lots of researchers don’t pay much attention to these layers. These layers can be used especially when you find some of the more sophisticated ones that tend to stick around for longer periods of time. While probably not as useful as tracking an actor to a backend system, these malware artifacts can provide valuable clues, serving as tools, techniques and procedures (TTPs) in tracking the ongoing operations of a specific threat actor across a wide range of operations and groups. In this case, we focus on MAN1, a sophisticated crypter dating back to 2014 that's still in use today.

Comments: 24 Pages. Malware Research; PE Cryptor

Download: PDF

Submission history

[v1] 2019-02-14 08:24:08