

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

Archived: 2026-04-05 18:07:30 UTC

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

Unique-IP document downloads: 688 times

Vixra.org is a pre-print repository rather than a journal. Articles hosted may not yet have been verified by peer-review and should be treated as preliminary. In particular, anything that appears to include financial or legal advice or proposed medical treatments should be treated with due caution. Vixra.org will not be responsible for any consequences of actions that result from any form of use of any documents on this website.

Add your own feedback and questions here:

You are equally welcome to be positive or negative about any paper but please be polite. If you are being critical you must mention at least one specific error, otherwise your comment will be deleted as unhelpful.

Source: <https://vixra.org/abs/1902.0257>