Malware Analysis - ROKRAT Unpacking from Injected Shellcode

Published: 2017-12-03 · Archived: 2026-04-05 18:41:44 UTC

The newest ROKRAT variant injects its shellcode into cmd.exe, which will in turn decrypt a PE image. We debug the injected code to obtain the payload. The sample is from an article published by Warren Mercer and Paul Rascagneres on talosintelligence.com (link below). …

...mer
