

MALWARE Analysis with Wireshark // TRICKBOT Infection

Published: 2022-05-05 · Archived: 2026-04-05 15:00:36 UTC

MALWARE Analysis with Wireshark // TRICKBOT Infection

2 903Gilla-markeringar

69 776Visningar

20225 maj

Download the pcap here and follow along: <https://malware-traffic-analysis.net/...> The password to unzip the file is "infected" If you liked this video, I'd really appreciate you giving me a like and subscribing, it helps me a whole lot. Also don't be shy, chat it up in the comments! Video for configuring GeoIP in Wireshark:

• [Map IP Address Locations with Wireshark \(U...](#) // Contact Me // LinkedIn: [/cgreer](#) YouTube: [/chrisgreer](#) Twitter: [/packetpioneer](#) == More On-Demand Training from Chris == ► Getting Started with Wireshark - <https://bit.ly/udemywireshark> ► Getting Started with Nmap - <https://bit.ly/udemynmap> == Live Wireshark Training == ► TCP/IP Deep Dive Analysis with Wireshark - <https://bit.ly/virtualwireshark> == Private Wireshark Training == Let's get in touch - <https://packetpioneer.com/product/pri...> Links above contain affiliate links where I will receive a small amount for any goods purchased. I thank you for clicking because it really helps to support me!! [0:00](#) Intro [0:48](#) DNS Filters [2:00](#) HTTP Requests/Replies [5:00](#) Using GeoIP [5:48](#) Exporting Usernames and Passwords [6:48](#) Exporting System Info [8:50](#) Extracting Hidden EXE Files [11:44](#) TLS Handshake Signatures

Följ med i transkriptionen.

[Chris Greer](#)

[172 000 prenumeranter](#)

Source: <https://www.youtube.com/watch?v=Brx4cygfm8>