[2] Lokibot analyzing - spoofing GULoader and LokiBot C2 [part2] - INetSim + BurpSuite

Published: 2021-08-22 · Archived: 2026-04-05 17:56:05 UTC

In case the C2 becomes unreachable/down and we have the served payload, we can reimplement C2 functionality. In this Video we are reimplementing the C2 of GULoader and LokiBot using 2 VMs and tools INetSim + BurpSuite. This is universal solution, very useful in most of situations. Remnux VM is Default Gateway for Window VM victim. Inetsim is simulating DNS, HTTP, HTTPS etc... Burpsuit is listening HTTPS/HTTP, for TLS it is generating Certificates on the fly according the requested host and redirecting to inetsim. Walk-Through: https://github.com/Dump-GUY/Malware-a...
