MALPITY: Automatic Identification and Exploitation of Tarpit Vulnerabilities in Malware

Submitted by grigby1 on Fri, 08/14/2020 - 11:44am

Title	MALPITY: Automatic Identification and Exploitation of Tarpit Vulnerabilities in Malware
Publication Type	Conference Paper
Year of Publication	2019
Authors	Walla, Sebastian, Rossow, Christian
Conference Name	2019 IEEE European Symposium on Security and Privacy (EuroS P)
Keywords	APIs, application program interfaces, application programming interface, Botnet , botnet infrastructures, botnets, command and control systems, compositionality, Dynamic Malware Analysis, Engines, global malware operations, Grippers, invasive software, law enforcement agencies, MALPITY, Malware, malware authors, malware families, malware spreading, malware tarpits, monetization techniques, network operation, network service, orthogonal defense, POSIX, pubcrawl, resilience, Resiliency, Servers, Sinkholing, Socket API, sockets, Tarpit, tarpit vulnerabilities, Unix, Winsock socket APIs

Abstract

Law enforcement agencies regularly take down botnets as the ultimate defense against global malware operations. By arresting malware authors, and simultaneously infiltrating or shutting down a botnet's network infrastructures (such as C2 servers), defenders stop global threats and mitigate pending infections. In this paper, we propose malware tarpits, an orthogonal defense that does not require seizing botnet infrastructures, and at the same time can also be used to slow down malware spreading and infiltrate its monetization techniques. A tarpit is a network service that causes a client to stay busy with a network operation. Our work aims to automatically identify network operations used by malware that will block the malware either forever or for a significant amount of time. We describe how to non-intrusively exploit such tarpit vulnerabilities in malware to slow down or, ideally, even stop malware. Using dynamic malware analysis, we monitor how malware interacts with the POSIX and Winsock socket APIs. From this, we infer network operations that would have blocked when provided certain network inputs. We augment this vulnerability search with an automated generation of tarpits that exploit the identified vulnerabilities. We apply our prototype MALPITY on six popular malware families and discover 12 previously-unknown tarpit vulnerabilities, revealing that all families are susceptible to our defense. We demonstrate how to, e.g., halt Pushdo's DGA-based C2 communication, hinder SalityP2P peers from receiving commands or updates, and stop Bashlite's spreading engine.

DOI 10.1109/EuroSP.2019.00049

Citation Key walla_malpity_2019

Engines Servers pubcrawl resilience Resiliency malware invasive software APIs application program interfaces Dynamic Malware Analysis Compositionality network service network operation botnet sockets Grippers botnet infrastructures botnets command and control systems global malware operations law enforcement agencies MALPITY malware authors malware families malware spreading malware tarpits monetization techniques orthogonal defense POSIX Sinkholing Socket API Tarpit tarpit vulnerabilities Unix Winsock socket APIs application programming interface