

Hackers get stuck in an evolving honeypot

August 6 2019, by David Bradley



Credit: CC0 Public Domain

Malware, malicious software, is on the rise, whether in the form of Trojans, worms, and viruses, bot-net systems, denial of service tools, and hacking programs. Antivirus, firewall, and intrusion detection systems are all essential components of the protections a systems operator might put in place on their users' computers and the network they operate.

Unfortunately, these are passive rather than active protections and so there are limitations to how well they can protect digital resources especially given the dynamic and evolving nature of attacks on seemingly robust systems.

Writing in the *International Journal of High Performance Computing and Networking*, researchers in China offer a somewhat novel paradigm—an evolving protection system that mimics the dynamics between predator and prey in the natural world.

Leyi Shi, Yuwen Cui, Xu Han, Honglong Chen, and Deli Liu of the China University of Petroleum (East China) in Qingdao, present a novel concept of a mimicry honeypot. This, they suggest, can bewilder adversaries (hackers and malware exploits) by evolving protective systems as network circumstances change when under attack. The team says that in tests their mimicry honeypot performs better than a conventional decoy system that might be in place on a network to attract and so distract [malware](#) and hackers away from the actual target. Fundamentally, the evolving honeypot adapts and so is never revealed as a honeypot, or honey-trap, to the attackers.

More information: Deli Liu et al. Mimicry honeypot: an evolutionary decoy system, *International Journal of High Performance Computing and Networking* (2019). [DOI: 10.1504/IJHPCN.2019.10022735](https://doi.org/10.1504/IJHPCN.2019.10022735)

Provided by Inderscience

Citation: Hackers get stuck in an evolving honeypot (2019, August 6) retrieved 18 April 2024 from <https://techxplore.com/news/2019-08-hackers-stuck-evolving-honeypot.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private

study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.