LevelBlue - Open Threat Exchange

By Garrett

Archived: 2026-04-05 22:04:37 UTC

For the last five years Trustwave has been monitoring a threat across a number of forensic cases that we have dubbed "Cherry Picker". This targeted Point of Sale (PoS) memory scraper has enjoyed a very low detection rate in the wild for quite some time. Cherry Picker uses a new memory scraping algorithm, a file infector for persistence, and cleaner malware that removes all traces of the infection from target systems. This sophisticated functionality and highly targeted victims have helped the malware remain under the radar of many AV and security companies. This post will expose the functionality of Cherry Picker and hopefully help organizations provide protection from this threat.
