LevelBlue - Open Threat Exchange

By TheNewRaikage

Archived: 2026-04-05 20:05:53 UTC

FileHash-MD5: 1 | **FileHash-SHA1:** 1 | **FileHash-SHA256:** 1 | **YARA:** 1 | **Domain:** 1

Yet another new credit card dumping utility has been discovered. BernhardPOS is named after (presumably) it's author who left in the build path of "C:\bernhard\Debug\bernhard.pdb" and also uses the name Bernhard in creating the mutex "OPSEC_BERNHARD". This utility does several interesting things to evade antivirus detection. We'll talk over some of them in detail. Details about the sample, including a hash are available at the end of this writeup.
