# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:17:29 UTC



## Tool: Decebal

| | |
|---|---|
| Names | Decebal |
| Category | Malware |
| Type | POS malware, Reconnaissance, Credential stealer |
| Description | (Trend Micro) Decebal refers to a PoS RAM scraper malware family first discovered at the beginning of 2014. Decebal is unique in that it is coded in VBScript and is compiled into an executable file. Most PoS RAM scrapers are coded in C, C++, or Delphi. Like BlackPOS, Decebal's source code was also leaked online. Decebal comes with many existing functionality found in established and even new PoS RAM scraper malware families |
| Information | <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf> <https://community.softwaregrp.com/t5/Security-Research/POS-malware-a-look-at-Dexter-and-Decebal/ba-p/272157> <https://www.fireeye.com/blog/threat-research/2014/10/data-theft-in-aisle-9-a-fireeye-look-at-threats-to-retailers.html> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.decebal> |

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

### All groups using tool Decebal

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **Unknown groups** | | | | |
| | _[ Interesting malware not linked to an actor yet ]_ | | | |

*1 group listed (0 APT, 0 other, 1 unknown)*