# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:05:41 UTC



## Tool: TreasureHunter

| | |
|---|---|
| Names | TreasureHunter<br>TREASUREHUNT<br>huntpos |
| Category | Malware |
| Type | POS malware, Credential stealer |
| Description | (FireEye) In this article we examine TREASUREHUNT, POS malware that appears to have been custom-built for the operations of a particular “dump shop,” which sells stolen credit card data. TREASUREHUNT enumerates running processes, extracts payment card information from memory, and then transmits this information to a command and control server. |
| Information | <https://www.fireeye.com/blog/threat-research/2016/03/treasurehunt_a_cust.html><br><https://isc.sans.edu/diary/How+Malware+Generates+Mutex+Names+to+Evade+Detection/19429/><br><https://www.flashpoint-intel.com/blog/treasurehunter-source-code-leaked/><br><http://adelmas.com/blog/treasurehunter.php><br><https://blog.group-ib.com/majikpos_treasurehunter_malware> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.treasurehunter> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:treasurehunt> |

Last change to this tool card: 18 November 2022

Download this tool card in JSON format

### All groups using tool TreasureHunter

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

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

---