# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:28:58 UTC



## Tool: SHELLSWEEP

| | |
|---|---|
| Names | SHELLSWEEP |
| Category | Malware |
| Type | Info stealer |
| Description | (Mandiant) One unique publicly available utility the actor has used is a PHP webshell based on PhpSpy, which Mandiant tracks as SHELLSWEEP, which contained functionality to retrieve credit card information. |
| Information | <https://www.mandiant.com/resources/fin13-cybercriminal-mexico> |

Last change to this tool card: 26 December 2021

Download this tool card in JSON format

### All groups using tool SHELLSWEEP

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | FIN13 | [Unknown] | 2016 | |

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