# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:01:25 UTC



## Tool: RottenPotato

| | |
|---|---|
| Names | RottenPotato |
| Category | Exploits |
| Type | Backdoor |
| Description | (ClearSky) Local Privilege Escalation tool from Windows Service Accounts to SYSTEM. |
| Information | <https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf> |

Last change to this tool card: 19 April 2021

Download this tool card in JSON format

### All groups using tool RottenPotato

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Dalbit | | 2022 | |
| | Operation Harvest | | 2016 | |
| | Sandworm Team, Iron Viking, Voodoo Bear | | 2009-Dec 2024 | |
| | Volatile Cedar | | 2012-Early 2020 | |

*4 groups listed (4 APT, 0 other, 0 unknown)*

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=684ecfd4-e04f-4568-bf0e-74d7ceb40935