# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:13:29 UTC



## Tool: FIVEHANDS

| | |
|---|---|
| Names | FIVEHANDS<br>Thieflock |
| Category | Malware |
| Type | Ransomware, Big Game Hunting |
| Description | (FireEye) In January 2021, Mandiant observed a new ransomware deployed against a victim and assigned the name FIVEHANDS.<br><br>• Analysis of FIVEHANDS revealed high similarity to DeathRansom, sharing several features, functions, and coding similarities. Absent in FIVEHANDS is a language check, similar to HELLOKITTY<br>• Both DEATHRANSOM and FIVEHANDS drops a ransom note in all non-excluded directories |
| Information | <https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html><br><https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126a><br><https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126b><br><https://research.nccgroup.com/2021/06/15/handy-guide-to-a-new-fivehands-ransomware-variant/><br><https://www.crowdstrike.com/blog/new-ransomware-variant-uses-golang-packer/> |
| MITRE ATT&CK | <https://attack.mitre.org/software/S0618/> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.fivehands> |

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

### All groups using tool FIVEHANDS

| Changed | Name | Country | Observed |
|---|---|---|---|

## APT groups

| | | | | |
|---|---|---|---|---|
| | UNC2447 | [Unknown] | 2020 | |

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

---

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=15096d65-ae63-4e6a-be93-fec62675b087