

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:18:27 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool ShadowHammer

Tool: ShadowHammer

| | |
|-------------|---|
| Names | ShadowHammer DAYJOB |
| Category | Malware |
| Type | Backdoor |
| Description | (Kaspersky) A supply chain attack that leveraged ASUS Live Update software. |
| Information | < https://securelist.com/operation-shadowhammer/89992/ > < https://skylightcyber.com/2019/03/28/unleash-the-hash-shadowhammer-mac-list/ > < https://countercept.com/blog/analysis-shadowhammer-asus-attack-first-stage-payload/ > < https://blog.reversinglabs.com/blog/forging-the-shadowhammer > < https://www.vkremez.com/2019/03/lets-learn-dissecting-operation.html > |
| Malpedia | < https://malpedia.caad.fkie.fraunhofer.de/details/win.shadowhammer > |

Last change to this tool card: 14 May 2020

Download this tool card in [JSON](#) format

All groups using tool ShadowHammer

| Changed | Name | Country | Observed | |
|-------------------|------------------------|---|---------------|---|
| APT groups | | | | |
| | APT 41 |  | 2012-Jul 2025 |  |

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