# Threat Group Cards: A Threat Actor Encyclopedia





## Tool: SUDDENICON

| | |
|---|---|
| Names | SUDDENICON<br>3CX Backdoor |
| Category | Malware |
| Type | Downloader |
| Description | According to CrowdStrike, this backdoor was discovered being embedded in a legitimate, signed version of 3CXDesktopApp, and thus constitutes a supply chain attack. |
| Information | <https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.3cx_backdoor> |

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

### All groups using tool SUDDENICON

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Lazarus Group, Hidden Cobra, Labyrinth Chollima | | 2007-May 2025 | |

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