

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:35:23 UTC

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


↪ Tool: Tcp_transfer

| | |
|-------------|---|
| Names | Tcp_transfer |
| Category | Malware |
| Type | Tunneling |
| Description | <p>(Bitdefender) The executable binds to “0.0.0.0:8080” address and starts listening for local connection. For each incoming connection on the local address, it creates a new connection to the C&C and start receiving and sending the data.</p> <p>The goal of such tool is to bypass network restriction such that the compromised machines that are not connected directly to the internet can communicate with the C&C through another compromised machine that has an internet connection.</p> |
| Information | < https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf > |

Last change to this tool card: 06 January 2021

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

All groups using tool Tcp_transfer

| Changed | Name | Country | Observed |
|-------------------|----------------------------|---|----------|
| APT groups | | | |
| | FunnyDream |  | 2018 |

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=c15386a1-c3f9-4c8b-ac4d-47588edbef70>