# Threat Group Cards: A Threat Actor Encyclopedia





## Tool: Tickler

| | |
|---|---|
| Names | Tickler |
| Category | Malware |
| Type | Backdoor |
| Description | (Microsoft) Microsoft Threat Intelligence identified two samples of the Tickler malware, a custom multi-stage backdoor, that Peach Sandstorm deployed in compromised environments as recently as July 2024. The first sample was contained in an archive file named Network Security.zip alongside benign PDF files used as decoy documents. |
| Information | <https://www.microsoft.com/en-us/security/blog/2024/08/28/peach-sandstorm-deploys-new-custom-tickler-malware-in-long-running-intelligence-gathering-operations/> |

Last change to this tool card: 23 October 2024

Download this tool card in JSON format

### All groups using tool Tickler

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | APT 33, Elfin, Magnallium | | 2013-Apr 2024 | |

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