# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:43:01 UTC



## Tool: AdvisorsBot

| | |
|---|---|
| Names | AdvisorsBot |
| Category | Malware |
| Type | Downloader |
| Description | (Proofpoint) Beginning in May 2018, Proofpoint researchers observed a previously undocumented downloader dubbed AdvisorsBot appearing in malicious email campaigns. The campaigns appear to primarily target hotels, restaurants, and telecommunications, and are distributed by an actor we track as TA555. To date, we have observed AdvisorsBot used as a first-stage payload, loading a fingerprinting module that, as with Marap, is presumably used to identify targets of interest to further infect with additional modules or payloads. AdvisorsBot is under active development and we have also observed another version of the malware completely rewritten in PowerShell and .NET. |
| Information | <https://www.proofpoint.com/us/threat-insight/post/new-modular-downloaders-fingerprint-systems-part-2-advisorsbot> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.advisorsbot> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:AdvisorsBot> |

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

### All groups using tool AdvisorsBot

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | TA555 | [Unknown] | 2018 | |

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