# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:03:51 UTC



## Tool: XDDown

| | |
|---|---|
| Names | XDDown |
| Category | Malware |
| Type | Downloader |
| Description | (ESET) XDDown is nothing but a downloader – hence our chosen name. This architecture choice is quite different from what we see in other APT malware frameworks, which tend to be quite complex with a whole set of backdoor commands and a logging mechanism. On one hand, the XDSpy approach is easier to develop but, on the other hand, it is much less flexible for the operators as a new binary needs to be built, downloaded and executed to perform any action on the compromised machine. |
| Information | <https://vblocalhost.com/uploads/VB2020-Faou-Labelle.pdf> |

Last change to this tool card: 19 October 2020

Download this tool card in JSON format

### All groups using tool XDDown

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | XDSpy | [Unknown] | 2011-Jul 2024 | |

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