

Blue Lambert - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:19:36 UTC

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


Tool: Blue Lambert

| | |
|-------------|---|
| Names | Blue Lambert |
| Category | Malware |
| Type | Loader |
| Description | <p>(Threatpost) Analysis of Black Lambert also exposed Blue Lambert, a second stage malware attack against a Black Lambert victim. Blue Lambert also exposed a number of operation or victim codenames that reference popular culture, including DOUBLESIDED SCOOBYSNACK, FUNNELCAKE CARNIVAL, RINGTOSS CARNIVAL and others.</p> <p>The researchers also found Green Lambert, an older version of the Blue Lambert malware.</p> |
| Information | <p><https://threatpost.com/tools-used-by-lamberts-apt-found-in-vault-7-dumps/124900/> <https://securelist.com/unraveling-the-lamberts-toolkit/77990/></p> |

Last change to this tool card: 20 April 2020

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

All groups using tool Blue Lambert

| Changed | Name | Country | Observed |
|-------------------|--|---|----------|
| APT groups | | | |
| | ↳ Subgroup: Longhorn, The Lamberts |  | 2009 |

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