# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:14:12 UTC



## Tool: Kelihos

| | |
|---|---|
| Names | Kelihos<br>Waledac<br>Hlux |
| Category | Malware |
| Type | Botnet, Downloader |
| Description | (CrowdStrike) For several years, pump-and-dump stock scams, dating ruses, credential phishing, money mule recruitment and rogue online pharmacy advertisements were the most common spam themes. In 2017, however, Kelihos was frequently used to spread other malware such as Luminosity RAT, Zyklon HTTP, Neutrino, Nymaim, Gozi ISFB, Zeus Panda, Kronos, and TrickBot. It was also observed spreading ransomware families including Shade, Cerber, and FileCrypt2. |
| Information | <https://www.crowdstrike.com/blog/farewell-to-kelihos-and-zombie-spider/><br><https://www.crowdstrike.com/blog/inside-the-takedown-of-zombie-spider-and-the-kelihos-botnet/><br><https://www.wired.com/2017/04/fbi-took-russias-spam-king-massive-botnet/><br><https://www.cyberscoop.com/doj-kelihos-botnet-peter-levashov-severa/><br><https://en.wikipedia.org/wiki/Kelihos_botnet> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.kelihos><br><https://malpedia.caad.fkie.fraunhofer.de/details/win.hlux> |

Last change to this tool card: 16 May 2020

Download this tool card in JSON format

### All groups using tool Kelihos

| Changed | Name | Country | Observed |
|---|---|---|---|

## Other groups

| | | | | |
|---|---|---|---|---|
| | Zombie Spider |  | 2010-Jun 2021 |  |

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

---

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=249447a1-e003-487a-a089-4d79aa1cde84