# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:04:39 UTC

## Tool: Vawtrak

| | |
|---|---|
| Names | Vawtrak<br>Catch<br>grabnew<br>NeverQuest |
| Category | Malware |
| Type | Banking trojan, Info stealer, Credential stealer, Botnet |
| Description | (Sophos) Vawtrak is an information stealing malware family that is primarily used to gain unauthorised access to bank accounts through online banking websites. Machines infected by Vawtrak form part of a botnet that collectively harvests login credentials for the online accounts to a wide variety of financial and other industry organisations. These stolen credentials are used, in combination with injected code and by proxying through the victim's machine, to initiate fraudulent transfers to bank accounts controlled by the Vawtrak botnet administrators. |
| Information | <https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-vawtrak-international-crimeware-as-a-service-tpna.pdf><br><https://www.kaspersky.com/blog/neverquest-trojan-built-to-steal-from-hundreds-of-banks/3247/><br><https://www.blueliv.com/downloads/network-insights-into-vawtrak-v2.pdf><br><https://info.phishlabs.com/blog/the-unrelenting-evolution-of-vawtrak><br><https://threatpost.com/pos-attacks-net-crooks-20-million-stolen-bank-cards/117595/><br><https://www.fidelissecurity.com/threatgeek/2016/05/vawtrak-trojan-bank-it-evolving><br><http://thehackernews.com/2017/01/neverquest-fbi-hacker.html><br><https://blog.fox-it.com/2018/08/09/bokbot-the-rebirth-of-a-banker/><br><https://www.proofpoint.com/us/threat-insight/post/In-The-Shadows><br><https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/><br><https://lokalhost.pl/gozi_tree.txt> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.vawtrak> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:vawtrak> |

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

### All groups using tool Vawtrak

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | FIN6, Skeleton Spider | [Unknown] | 2015-Oct 2021 | |
| **Other groups** | | | | |
| | Lunar Spider | | 2019 | |

*2 groups listed (1 APT, 1 other, 0 unknown)*

↑

---