# Poison Ivy - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:43:21 UTC



## Tool: Poison Ivy

| | |
|---|---|
| Names | Poison Ivy<br>pivy<br>poisonivy<br>Gen:Trojan.Heur.PT<br>Darkmoon<br>Chymine<br>SPIVY |
| Category | Malware |
| Type | Reconnaissance, Backdoor, Info stealer, Credential stealer, Exfiltration |
| Description | Poison Ivy is a popular remote access tool (RAT) that has been used by many groups. |
| Information | <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf><br><https://www.fortinet.com/blog/threat-research/deep-analysis-of-new-poison-ivy-variant.html><br><https://blog.fortinet.com/2017/09/15/deep-analysis-of-new-poison-ivy-plugx-variant-part-ii><br><http://contagiodump.blogspot.com/2010/01/jan-17-trojan-darkmoonb-exe-haiti.html><br><https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/august/analysing-a-recent-poison-ivy-sample/><br><https://researchcenter.paloaltonetworks.com/2016/04/unit42-new-poison-ivy-rat-variant-targets-hong-kong-pro-democracy-activists/><br><https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html><br><https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html><br><https://researchcenter.paloaltonetworks.com/2014/09/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/><br><http://blogs.360.cn/post/APT_C_01_en.html><br><https://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/> |

| | |
|---|---|
| MITRE ATT&CK | <https://attack.mitre.org/software/S0012/> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.poison_ivy><br><https://malpedia.caad.fkie.fraunhofer.de/details/win.darkmoon> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:Poison%20Ivy> |

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

### All groups using tool Poison Ivy

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Anchor Panda, APT 14 | | 2012 | |
| | APT 6 | | 2011 | |
| | APT 17, Deputy Dog, Elderwood, Sneaky Panda | | 2009-Jun 2024 | |
| | APT 20, Violin Panda | | 2014-2017 | |
| | Axiom, Group 72 | | 2008-2008/2014 | |
| | Bookworm | | 2015 | |
| | Comment Crew, APT 1 | | 2006-May 2018 | |
| | DragonOK | | 2015-Jan 2017 | |
| | Dust Storm | | 2010 | |
| | Gallium | | 2018-Jun 2022 | |
| | IronHusky | | 2017-Aug 2021 | |
| | Moafee | | 2014 | |
| | Molerats, Extreme Jackal, Gaza Cybergang | [Gaza] | 2012-Jul 2023 | |
| | Mustang Panda, Bronze President | | 2012-Jun 2025 | |

| | | | | |
|---|---|---|---|---|
| | Nightshade Panda, APT 9, Group 27 | | 2013-Sep 2016 | |
| | Nitro, Covert Grove | | 2011-Jul 2014 | |
| | PittyTiger, Pitty Panda | | 2011-2014 | |
| | RedDelta | | 2020-Jul 2023 | |
| | RedFoxtrot | | 2014-Aug 2021 | |
| | Siesta | | 2014 | |
| | Space Pirates | | 2017-Nov 2024 | |
| | Stone Panda, APT 10, menuPass | | 2006-Mar 2025 | |
| | TA428 | | 2013-Jan 2022 | |
| | Temper Panda, admin@338 | | 2014 | |
| | Tropic Trooper, Pirate Panda, APT 23, KeyBoy | | 2011-Jun 2023 | |

*25 groups listed (25 APT, 0 other, 0 unknown)*

---

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f0250d37-fcad-40db-bfa4-adb597d651db