# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:39:00 UTC



## Tool: PyXie

| | |
|---|---|
| Names | PyXie<br>PyXie RAT |
| Category | Malware |
| Type | Backdoor, Loader |
| Description | (BlackBerry) PyXie has been deployed in an ongoing campaign that targets a wide range of industries. It has been seen in conjunction with Cobalt Strike beacons as well as a downloader that has similarities to the Shifu banking Trojan. Analysts have observed evidence of the threat actors attempting to deliver ransomware to the healthcare and education industries with PyXie.<br><br>Key highlights of the PyXie campaign include:<br>• Legitimate LogMeIn and Google binaries used to sideload payloads.<br>• A Trojanized Tetris app to load and execute Cobalt Strike stagers from internal network shares.<br>• Use of a downloader with similarities to Shifu named 'Cobalt Mode'.<br>• Use of SharpHound to collect active directory information from victims.<br>• A custom compiled Python interpreter that uses scrambled opcodes to hinder analysis.<br>• Use of a modified RC4 algorithm to encrypt payloads with a unique key per infected host. |
| Information | <https://blogs.blackberry.com/en/2019/12/meet-pyxie-a-nefarious-new-python-rat> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.pyxie> |

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

### All groups using tool PyXie

| Changed | Name | Country | Observed |
|---|---|---|---|
| **APT groups** | | | |

| | | | | |
|---|---|---|---|---|
| | Sprite Spider, Gold Dupont | [Unknown] | 2015-Nov 2022 | |

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

---

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=4e675551-3b29-4764-819b-0b8b68e3dcb4