

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:36:35 UTC

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





## Tool: PupyRAT

Names	PupyRAT Pupy pupy
Category	<a href="#">Tools</a>
Type	<a href="#">Backdoor</a>
Description	Pupy is an open-source, cross-platform RAT and post-exploitation framework mainly written in python. Pupy can be loaded from various loaders, including PE EXE, reflective DLL, Linux ELF, pure python, powershell and APK. Most of the loaders bundle an embedded python runtime, python library modules in source/compiled/native forms as well as a flexible configuration. They bootstrap a python runtime environment mostly in-memory for the later stages of pupy to run in. Pupy can communicate using various transports, migrate into processes, load remote python code, python packages and python C-extensions from memory.
Information	<p>&lt;<a href="https://www.secureworks.com/blog/iranian-pupyrat-bites-middle-eastern-organizations">https://www.secureworks.com/blog/iranian-pupyrat-bites-middle-eastern-organizations</a>&gt;</p> <p>&lt;<a href="https://blog.cyber4sight.com/2017/02/malicious-powershell-script-analysis-indicates-shamoon-actors-used-pupy-rat/">https://blog.cyber4sight.com/2017/02/malicious-powershell-script-analysis-indicates-shamoon-actors-used-pupy-rat/</a>&gt;</p> <p>&lt;<a href="https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html">https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html</a>&gt;</p> <p>&lt;<a href="https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/">https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/</a>&gt;</p> <p>&lt;<a href="https://github.com/n1nj4sec/pupy">https://github.com/n1nj4sec/pupy</a>&gt;</p> <p>&lt;<a href="https://labs.k7computing.com/index.php/pupy-rat-hiding-under-werfaults-cover/">https://labs.k7computing.com/index.php/pupy-rat-hiding-under-werfaults-cover/</a>&gt;</p> <p>&lt;<a href="https://asec.ahnlab.com/en/64258/">https://asec.ahnlab.com/en/64258/</a>&gt;</p>
MITRE ATT&CK	< <a href="https://attack.mitre.org/software/S0192/">https://attack.mitre.org/software/S0192/</a> >
Malpedia	<p>&lt;<a href="https://malpedia.caad.fkie.fraunhofer.de/details/elf.pupy">https://malpedia.caad.fkie.fraunhofer.de/details/elf.pupy</a>&gt;</p> <p>&lt;<a href="https://malpedia.caad.fkie.fraunhofer.de/details/py.pupy">https://malpedia.caad.fkie.fraunhofer.de/details/py.pupy</a>&gt;</p> <p>&lt;<a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.pupy">https://malpedia.caad.fkie.fraunhofer.de/details/win.pupy</a>&gt;</p>

Last change to this tool card: 22 April 2024

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

### All groups using tool PupyRAT

Changed	Name	Country	Observed	
<b>APT groups</b>				
	<a href="#">APT 33, Elfin, Magnallium</a>		2013-Apr 2024	
	<a href="#">Cutting Kitten, TG-2889</a>		2012-Mar 2016	●
	<a href="#">LightBasin</a>		2016	
	<a href="#">Magic Hound, APT 35, Cobalt Illusion, Charming Kitten</a>		2012-Jun 2025	●

4 groups listed (4 APT, 0 other, 0 unknown)

---

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7b6db856-4677-46f4-b422-1272cbb8c783>