PyVil RAT - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 12:15:14 UTC

Tool: PyVil RAT

Names	PyVil RAT PyVil
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Credential stealer, Keylogger, Downloader, Exfiltration
Description	(Cybereason) PyVil RAT possesses different functionalities, and enables the attackers to exfiltrate data, perform keylogging and the taking of screenshots, and the deployment of more tools such as LaZagne in order to steal credentials. The PyVil RAT has several functionalities including: • Keylogger • Running cmd commands • Taking screenshots • Downloading more Python scripts for additional functionality • Dropping and uploading executables • Opening an SSH shell • Collecting information such as: o Anti-virus products installed o USB devices connected o Chrome version
Information	<https://www.cybereason.com/blog/no-rest-for-the-wicked-evilnum-unleashes-pyvil-rat>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/py.pyvil>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:PyVil%20RAT>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool PyVil RAT

Changed	Name	Country	Observed	
APT groups				
	Evilnum	[Unknown]	2018-2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=d1f93996-93c1-43a8-9893-2d2735fa1023