Peppy RAT - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:12:24 UTC

Tool: Peppy RAT

Names	Peppy RAT Peppy Trojan
Category	Malware
Type	Backdoor, Keylogger, Info stealer, Downloader, Exfiltration
Description	(Proofpoint) Peppy is a Python-based RAT with the majority of its appearances having similarities or definite overlap with MSIL/Crimson RAT appearances. Peppy communicates to its C&C over HTTP and utilizes SQLite for much of its internal functionality and tracking of exfiltrated files. The primary purpose of Peppy may be the automated exfiltration of potentially interesting files and keylogs. Once Peppy successfully communicates to its C&C, the keylogging and exfiltration of files using configurable search parameters begins. Files are exfiltrated using HTTP POST requests. In addition to keylogging and the exfiltration of files, Peppy is also capable of accepting commands from its C&C to update itself, disable itself, exfiltrate a specific file, uninstall itself, execute a shell command, take screenshots, spawn a reverse shell, and download a remote file and execute it.
Information	<https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.peppy_rat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Peppy%20RAT>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool Peppy RAT

Changed	Name	Country	Observed

APT groups

	Transparent Tribe, APT 36		2013-Mar 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=23a7f4a8-9826-47a8-a7e8-1c4da9f44ca6