GUP Proxy Tool - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:50:35 UTC

Tool: GUP Proxy Tool

Names	GUP Proxy Tool
Category	Malware
Type	Backdoor
Description	(Proofpoint) The GUP command and control proxy tool may impersonate the name of a piece of legitimate opensource software available at wingup[.]org, which is used by Notepad++. In historic campaigns by APT adversaries, legitimate GUP.exe versions were utilized that were digitally signed by Notepad++. In this campaign, files appeared to impersonate the GUP.exe file name rather than being a legitimate signed binary. The function of this tool is to set up a TCP listener on a localhost, receive encoded data via requests from the SodomNormal localhost module, and to forward this data to the command and control IP via HTTP. The GUP Proxy Tool has a hardcoded configuration which is included as both strings and integers.
Information	<https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.gup_proxy>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool GUP Proxy Tool

Changed	Name	Country	Observed	
APT groups				
	LookBack, TA410	[Unknown]	2019-Feb 2022	

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