Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:28:27 UTC

Tool: Upatre

Names	Upatre
Category	Malware
Type	Botnet, Downloader
Description	(Palo Alto) First discovered in 2013, Upatre is primarily a downloader tool responsible for delivering additional trojans onto the victim host. It is most well-known for being tied with the Dyre banking trojan, with a peak of over 250,000 Upatre infections per month delivering Dyre back in July 2015.
Information	<https://unit42.paloaltonetworks.com/unit42-upatre-continues-evolve-new-anti-analysis-techniques/> <https://johannesbader.ch/2015/06/Win32-Upatre-BI-Part-1-Unpacking/> <https://secrary.com/ReversingMalware/Upatre/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.upatre>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Upatre>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool Upatre

Changed	Name	Country	Observed	
APT groups				
	Wizard Spider, Gold Blackburn		2014-May 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=4004b735-cd87-4a1b-b677-042509d11ab3