Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:19:27 UTC

Tool: Vatet

Names	Vatet
Category	Malware
Type	Loader
Description	(Palo Alto) Vatet is a custom loader that executes XOR encoded shellcode from the local disk or a network share. The loaders are typically open source applications found on GitHub, or other repositories, that the actors modify to load their shellcode. In most cases, the payload winds up being Cobalt Strike beacons and/or stagers, but some of the more recent payloads have been an updated version of the PyXie RAT. Vatet is often a precursor to enterprise-wide ransomware attacks.
Information	<https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/> <https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/>

Last change to this tool card: 23 April 2021

Download this tool card in JSON format

All groups using tool Vatet

Changed	Name	Country	Observed	
APT groups				
	Sprite Spider, Gold Dupont	[Unknown]	2015-Nov 2022	

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