Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:57:13 UTC

Tool: Xbash

Names	Xbash
Category	Malware
Type	Ransomware, Miner, Botnet
Description	Xbash is a malware family that has targeted Linux and Microsoft Windows servers. The malware has been tied to the Iron Group, a threat actor group known for previous ransomware attacks. Xbash was developed in Python and then converted into a self-contained Linux ELF executable by using PyInstaller.
Information	<https://unit42.paloaltonetworks.com/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0341/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.xbash>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Xbash>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Xbash

Changed	Name	Country	Observed	
Other groups				
	Rocke, Iron Group		2018-Apr 2021	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=9bcbde25-5722-4fc3-8acc-6b9cd6a8a939