Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:03:24 UTC

Tool: Ketrum

Names	Ketrum
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Intezer) The three samples we discovered seem to be a mix of the Ketrican and Okrum backdoors documented by researchers at ESET in 2019. Features have been merged from these two malware families to create a different RAT class for the group. We've decided to call this umbrella of malware "Ketrum." The new samples we found continue the Ke3chang group's strategy of using a basic backdoor to gain control over the victim's device, so that an operator can then connect to it and run commands manually to conduct further operations.
Information	<https://www.intezer.com/blog/research/the-evolution-of-apt15s-codebase-2020/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ketrum>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:ketrum>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Ketrum

Changed	Name	Country	Observed	
APT groups				
	Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon		2010-Oct 2024	

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