Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:58:03 UTC

Tool: TidePool

Names	TidePool
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Palo Alto) TidePool contains many capabilities common to most RATs. It allows the attacker to read, write and delete files and folders, and run commands over named pipes. TidePool gathers information about the victim's computer, base64 encodes the data, and sends it to the Command and Control (C2) server via HTTP, which matches capabilities of the BS2005 malware family used by the Ke3chang actor.
Information	<https://unit42.paloaltonetworks.com/operation-ke3chang-resurfaces-with-new-tidepool-malware/> <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.tidepool>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:TidePool>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool TidePool

Changed	Name	Country	Observed	
APT groups				
	DragonOK		2015-Jan 2017	
	Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon		2010-Oct 2024	

2 groups listed (2 APT, 0 other, 0 unknown)
