Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:05:45 UTC

Tool: Combos

Names	Combos
Category	Malware
Type	Backdoor, Info stealer, Credential stealer, Exfiltration
Description	(AlienVault) The COMBOS malware family is an HTTP based backdoor. The backdoor is capable of file upload, file download, spawning a interactive reverse shell, and terminating its own process. The backdoor may decrypt stored Internet Explorer credentials from the local system and transmit the credentials to the C2 server. The COMBOS malware family does not have any persistence mechanisms built into itself.
Information	<https://otx.alienvault.com/pulse/56aa5a8d67db8c6aafe00db7>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.combos>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Combos

Changed	Name	Country	Observed	
APT groups				
	Comment Crew, APT 1		2006-May 2018	

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