Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:15:48 UTC

Tool: Rambo

Names	Rambo brebsd
Category	Malware
Type	Reconnaissance, Backdoor
Description	(securitykitten) Rambo is a unique backdoor with features that are the result of some odd design decisions. In the initial dropper the configuration containing offsets and filenames are encoded with TEA, however the binaries are not encoded at all. It uses AES to encode the host information that is sent out over the network, however the C2 is hidden with a single byte XOR. While they may not make much sense to a reverse engineer, it gives some idea to the information that the author doesn't want to be easily recovered. By writing commands to temporary files and trying to communicate between multiple processes, the authors turn a simple stage 1 implant into something that is confusing and more difficult to study.
Information	<https://talos-intelligence-site.s3.amazonaws.com/production/document_files/files/000/000/062/original/RamboDIMVA2016.pdf> <https://securitykitten.github.io/2017/02/15/the-rambo-backdoor.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.rambo>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Rambo

Changed	Name	Country	Observed	
APT groups				
	DragonOK		2015-Jan 2017	

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