Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:32:49 UTC

Tool: Seasalt

Names	Seasalt
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	The SEASALT malware family communicates via a custom binary protocol. It is capable of gathering some basic system information, file system manipulation, file upload and download, process creation and termination, and spawning an interactive reverse shell. The malware maintains persistence by installing itself as a service.
Information	<https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf> <http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0345/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.seasalt>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:seasalt>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Seasalt

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

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