Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:41:23 UTC

Tool: SodaMaster

Names	SodaMaster DelfsCake dfls DARKTOWN HEAVYPOT
Category	Malware
Type	Backdoor, Downloader, Loader
Description	(Kaspersky) Another payload of the Ecipekac loader, which we call SodaMaster (a.k.a DelfsCake), is also a new fileless malware. In our research we found more than 10 samples of SodaMaster. All the collected samples of this module were almost identical, with the offsets and hex patterns of all functions perfectly matching. The only differences were in the configuration data, including a hardcoded C2, an encoded RSA key and additional data for calculating a mutex value.
Information	<https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/> <https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_202_niwa-yanagishita_en.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0627/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sodamaster>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool SodaMaster

Changed	Name	Country	Observed
APT groups			

	Stone Panda, APT 10, menuPass		2006-Mar 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=583bd930-612c-400d-b0c0-ac4ec05023b0