Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:08:22 UTC

Tool: Salgorea

Names	Salgorea BadCake
Category	Malware
Type	Reconnaissance, Backdoor
Description	(Accenture) This backdoor is commonly dropped by either an SFX or an exploit document (e.g. Microsoft Corp. Word or PDF file). Some of this backdoor's observed capabilities include: • Arbitrary file, process and registration creation • Fingerprinting the local machine • Running arbitrary shellcode Once dropped, it is usually divided into multiple components in order to be side-loaded, in a fashion similar to other remote access tools including PlugX and NetTraveler.
Information	<https://www.accenture.com/us-en/blogs/blogs-pond-loach-delivers-badcake-malware>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.salgorea>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Salgorea

Changed	Name	Country	Observed	
APT groups				
	APT 32, OceanLotus, SeaLotus		2013-Aug 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a4e1fbba-2e37-453c-b688-420e2bb03cdd