Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:25:23 UTC

Tool: CAKETAP

Names	CAKETAP
Category	Malware
Type	Rootkit
Description	(Mandiant) CAKETAP is a kernel module rootkit that UNC2891 deployed on key server infrastructure running Oracle Solaris. CAKETAP can hide network connections, processes, and files. During initialization, it removes itself from the loaded modules list and updates the last_module_id with the previously loaded module to hide its presence.
Information	<https://www.mandiant.com/resources/unc2891-overview>

Last change to this tool card: 03 April 2022

Download this tool card in JSON format

All groups using tool CAKETAP

Changed	Name	Country	Observed	
APT groups				
	UNC2891	[Unknown]	2020	

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