Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:03:49 UTC

Tool: SUN4ME

Names	SUN4ME
Category	Malware
Type	Reconnaissance
Description	(Mandiant) UNC2891 had deployed different versions of an extensive toolkit which appears to be developed under the name SUN4ME. SUN4ME contains tools for network reconnaissance, host enumeration, exploitation of known vulnerabilities, log wiping, file operations, as well as common shell utilities.
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 SUN4ME

Changed	Name	Country	Observed	
APT groups				
	UNC2891	[Unknown]	2020	

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