Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:15:24 UTC

Tool: WINGHOOK

Names	WINGHOOK
Category	Malware
Type	Credential stealer
Description	(Mandiant) WINGHOOK is a keylogger for Linux and Unix based operating systems. It is packaged as a shared library (SO file) that hooks the read and fgets functions, which are two common functions used for processing user input. The captured data is stored in an encoded format in the directory /var/tmp/ with a filename that begins with .zmanDw.
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 WINGHOOK

Changed	Name	Country	Observed	
APT groups				
	UNC2891	[Unknown]	2020	

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