Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:43:40 UTC

Tool: STEELHOUND

Names	STEELHOUND
Category	Malware
Type	Dropper
Description	(Mandiant) Mandiant discovered UNC2891 leveraging a similar (STEELCORGI) in-memory dropper that also used environment variables to decrypt its embedded payload but instead relied on RC4 encryption, we have named this STEELHOUND. In addition to functioning as dropper for an embedded payload, STEELHOUND is also able to encrypt new payloads by encrypting a target binary and writing it to disk along with a copy of itself and an end-of-file configuration.
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 STEELHOUND

Changed	Name	Country	Observed	
APT groups				
	UNC2891	[Unknown]	2020	

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