Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:19:35 UTC

Tool: SoreFang

Names	SoreFang
Category	Malware
Type	Downloader
Description	(NCSC-UK) Malware, dubbed 'SoreFang' by the NCSC, is a first stage downloader that uses HTTP to exfiltrate victim information and download second stage malware. The sample analysed by the NCSC contains the same infrastructure as a WellMess sample. It is likely that SoreFang targets SangFor devices.
Information	<https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf> <https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198a> <https://securelist.com/apt-trends-report-q3-2020/99204/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0516>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sorefang>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:SoreFang>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool SoreFang

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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