Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 15:41:17 UTC

Tool: BADFLICK

Names	BADFLICK
Category	Malware
Type	Backdoor
Description	(FireEye) BADFLICK, a backdoor that is capable of modifying the file system, generating a reverse shell, and modifying its command-and-control configuration.
Information	<https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html> <https://blog.amossys.fr/badflick-is-not-so-bad.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0642/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.badflick>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:BADFLICK>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool BADFLICK

Changed	Name	Country	Observed	
APT groups				
	Leviathan, APT 40, TEMP.Periscope		2013-Jul 2021	

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