Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:48:02 UTC

Tool: BADCALL

Names	BADCALL
Category	Malware
Type	Backdoor
Description	(US-CERT) This report provides analysis of four (4) malicious executable files. The first three (3) files are 32-bit Windows executables that function as proxy servers and implement a 'Fake TLS' method similar to the behavior described in a previously published NCCIC report, MAR-10135536-B. The fourth file is an Android Package Kit (APK) file designed to run on Android platforms as a fully functioning Remote Access Tool (RAT).
Information	<https://www.us-cert.gov/ncas/analysis-reports/ar19-252a>
MITRE ATT&CK	<https://attack.mitre.org/software/S0245/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.badcall> <https://malpedia.caad.fkie.fraunhofer.de/details/win.badcall>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:BADCALL>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool BADCALL

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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