Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:06:36 UTC

Tool: BUFFETLINE

Names	BUFFETLINE
Category	Malware
Type	Reconnaissance, Backdoor, Downloader, Exfiltration
Description	(US-CERT) This report looks at a full-featured beaconing implant. This sample uses PolarSSL for session authentication, but then utilizes a FakeTLS scheme for network encoding using a modified RC4 algorithm. It has the capability to download, upload, delete, and execute files; enable Windows CLI access; create and terminate processes; and perform target system enumeration.
Information	<https://www.us-cert.gov/ncas/analysis-reports/ar20-045f>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.buffetline>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:BUFFETLINE>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool BUFFETLINE

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

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