Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:22:37 UTC

Tool: TONEDEAF

Names	TONEDEAF
Category	Malware
Type	Reconnaissance, Backdoor, Tunneling, Info stealer, Exfiltration
Description	(FireEye) TONEDEAF is a backdoor that communicates with Command and Control servers using HTTP or DNS. Supported commands include system information collection, file upload, file download, and arbitrary shell command execution. Although this backdoor was coded to be able to communicate with DNS requests to the hard-coded Command and Control server, c[.]cdn-edge-akamai[.]com, it was not configured to use this functionality.
Information	<https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.tonedeaf>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:TONEDEAF>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool TONEDEAF

Changed	Name	Country	Observed	
APT groups				
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=fe0cfb06-ded6-4220-90c8-038cb2e88126