Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:51:14 UTC

Tool: SOUNDBITE

Names	SOUNDBITE Denis
Category	Malware
Type	Reconnaissance, Backdoor, Downloader, Tunneling, Exfiltration
Description	(FireEye) • C2 communications via DNS • Process creation • File upload • Shell command execution • File and directory enumeration/manipulation • Window enumeration • Registry manipulation • System information gathering
Information	<https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html> <https://securelist.com/use-of-dns-tunneling-for-cc-communications/78203/> <https://ruxcon.org.au/assets/2017/slides/bart-RuxCon-Presentation.pptx> <https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/SpyRATsofOceanLotusMalwareWhitePaper.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0354/> <https://attack.mitre.org/software/S0157/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.soundbite>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:SOUNDBITE>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool SOUNDBITE

Changed	Name	Country	Observed

APT groups

	APT 32, OceanLotus, SeaLotus		2013-Aug 2024	

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

↑

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=771e976f-81e0-4775-a542-9cdbd531713d