Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:58:13 UTC

Tool: Cuegoe

Names	Cuegoe
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Downloader
Description	(FireEye) • Command and control (C2) communications via TCP raw sockets • Four configured C2s and six configured ports – randomly-chosen C2/port for communications • Registry manipulation • Get the current module's file name • Gather system information including registry values, user name, computer name, and current code page • File system interaction including directory creation, file deletion, reading, and writing files • Load additional modules and execute code • Terminate processes • Anti-disassembly
Information	<https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html> <http://blog.malwaremustdie.org/2014/08/another-country-sponsored-malware.html> <https://www.eff.org/deeplinks/2014/01/vietnamese-malware-gets-personal>
MITRE ATT&CK	<https://attack.mitre.org/software/S0155/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cuegoe>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool Cuegoe

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=5c526664-bbfb-4310-914a-156c0d51622d