Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:15:52 UTC

Tool: LEOUNCIA

Names	LEOUNCIA shoco
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer
Description	(FireEye) Like Vinself, Leouncia is a powerful backdoor that is designed to take complete control over the infected machine. Similar to Vinself, Leouncia also uses HTTP to carry its custom obfuscated payload. I found Leouncia's obfuscation techniques far more sophisticated than what I found within Vinself. Moreover, Leouncia tries its best to hide its presence from signature based sensors. It generates its http communication randomly by using varying levels of system information in conjunction with Windows random number generation APIs. The result is that every instance of its C&C communication will be different from the previous one.
Information	<https://www.fireeye.com/blog/threat-research/2010/12/leouncia-yet-another-backdoor.html> <https://www.fireeye.com/blog/threat-research/2010/12/leouncia-yet-another-backdoor-part-2.html> <https://www.rsaconference.com/writable/presentations/file_upload/crwd-t11-hide_and_seek-how_threat_actors_respond_in_the_face_of_public_exposure.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.leouncia>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool LEOUNCIA

Changed	Name	Country	Observed
APT groups			

	APT 5, Keyhole Panda		2007-Aug 2019	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=660fc052-443f-4b96-8357-06b48255b32b