Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:25:12 UTC

Tool: BlackRock

Names	BlackRock AmpleBot
Category	Malware
Type	Reconnaissance, Backdoor, Banking trojan, Keylogger, Info stealer, Credential stealer, Exfiltration
Description	(ThreatFabric) Around May 2020 ThreatFabric analysts have uncovered a new strain of banking malware dubbed BlackRock that looked pretty familiar. After investigation, it became clear that this newcomer is derived from the code of the Xerxes banking malware, which itself is a strain of the LokiBot Android banking Trojan. The source code of the Xerxes malware was made public by its author around May 2019, which means that it is accessible to any threat actor. Technical aspects aside, one of the interesting differentiators of BlackRock is its target list; it contains an important number of social, networking, communication and dating applications. So far, many of those applications haven't been observed in target lists for other existing banking Trojans. It therefore seems that the actors behind BlackRock are trying to abuse the grow in online socializing that increased rapidly in the last months due to the pandemic situation. BlackRock offers a quite common set of capabilities compared to average Android banking Trojans. It can perform the infamous overlay attacks, send, spam and steal SMS messages, lock the victim in the launcher activity (HOME screen of the device), steal and hide notifications, deflect usage of Antivirus software on the device and act as a keylogger. Interestingly, the Xerxes Trojan itself offers more features, but it seems that actors have removed some of them in order to only keep those that they consider useful to steal personal information. Note: This malware was initially named BlackRock and later renamed to AmpleBot.
Information	<https://www.threatfabric.com/blogs/blackrock_the_trojan_that_wanted_to_get_them_all.html> <https://www.threatfabric.com/blogs/alien_the_story_of_cerberus_demise.html> <https://www.threatfabric.com/blogs/ermac-another-cerberus-reborn.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.amplebot>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool BlackRock

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=8d0ec018-69e1-4f6e-b7ef-b35e6a0dec39