body - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:49:43 UTC

Tool: Aria-body

Names	Aria-body AR
Category	Malware
Type	Reconnaissance, Backdoor, Keylogger, Info stealer, Tunneling
Description	(Check Point) The RAT includes rather common capabilities of a backdoor, including: • Create/Delete Files/Directories • Take a screenshot • Search file • Launch files using ShellExecute • Enumerate process loaded modules • Gather files' metadata • Gather TCP and UDP table status listing • Close a TCP session • Collect OS information • Verify location using checkip.amazonaws.com • (Optional) Inter-process pipe based communication Some of Aria-body variations also included other modules such as: • USB data gathering module • Keylogger module to collect raw input device-based keystrokes – added by February 2018 • Reverse socks proxy module – added by February 2018 • Loading extensions module – added by December 2019
Information	<https://research.checkpoint.com/2020/naikon-apt-cyber-espionage-reloaded/> <https://securelist.com/naikons-aria/96899/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0456/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ariabody>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Aria-body

Changed	Name	Country	Observed	
APT groups				
	Naikon, Lotus Panda		2010-Apr 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2fb2ec92-5ef7-44e5-b69c-3356ff2a328f