Aria-body loader - Threat Group Cards: A Threat Actor Encyclopedia

Tool: Aria-body loader

Names	Aria-body loader
Category	Malware
Type	Loader
Description	(Check Point) The functionality of the Aria-body loader has not changed significantly since 2017, but the implementation varied from version to version. This loader appears to be specifically created for the Aria-body backdoor. Overall, the loader is responsible for the following tasks: • Establish persistence via the Startup folder or theRun registry key (some variants). • Inject itself to another process such as rundll32.exe and dllhost.exe (some variants). • Decrypt two blobs: Import Table and the loader configuration. • Utilize a DGA algorithm if required. • Contact the embedded / calculated C&C address in order to retrieve the next stage payload. • Decrypt the received payload DLL (Aria-body backdoor). • Load and execute an exported function of the DLL – calculated using djb2 hashing algorithm.
Information	<https://research.checkpoint.com/2020/naikon-apt-cyber-espionage-reloaded/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ariabody>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool Aria-body loader

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=5eaa1038-46a4-4d05-8982-25ef7e1cf077