Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:07:19 UTC

Tool: LIONTAIL

Names	LIONTAIL
Category	Malware
Type	Loader
Description	(Check Point) In the latest campaign, the threat actor leveraged the LIONTAIL framework, a sophisticated set of custom loaders and memory resident shellcode payloads. LIONSTAIL's implants utilize undocumented functionalities of the HTTP.sys driver to extract payloads from incoming HTTP traffic. Multiple observed variants of LIONTAIL-associated malware suggest Scarred Manticore generates a tailor-made implant for each compromised server, allowing the malicious activities to blend into and be undiscernible from legitimate network traffic.
Information	<https://research.checkpoint.com/2023/from-albania-to-the-middle-east-the-scarred-manticore-is-listening/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.liontail>

Last change to this tool card: 17 January 2024

Download this tool card in JSON format

All groups using tool LIONTAIL

Changed	Name	Country	Observed	
APT groups				
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	

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