Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:12:12 UTC

Tool: Owowa

Names	Owowa
Category	Malware
Type	Credential stealer
Description	(Kaspersky) While looking for potentially malicious implants that targeted Microsoft Exchange servers, we identified a suspicious binary that had been submitted to a multiscanner service in late 2020. Analyzing the code, we determined that the previously unknown binary is an IIS module, aimed at stealing credentials and enabling remote command execution from OWA. We named the malicious module ‘Owowa’, and identified several compromised servers located in Asia.
Information	<https://securelist.com/owowa-credential-stealer-and-remote-access/105219/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.owowa>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool Owowa

Changed	Name	Country	Observed	
APT groups				
	Gelsemium		2014-2023	

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