Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:58:15 UTC

Tool: IronWind

Names	IronWind
Category	Malware
Type	Backdoor
Description	(Proofpoint) Once sideloaded, IronWind sent an HTTP GET request to a known TA402 C2 domain. After receiving the HTTP GET request, the C2 responded with shellcode that represented the third stage of the infection chain. During Proofpoint's analysis, the shellcode used reflective .NET loaders to conduct WMI queries. The shellcode also served as a multipurpose loader, downloading the fourth stage—a .NET executable that used SharpSploit, a .NET post-exploitation library written in C#.
Information	<https://www.proofpoint.com/us/blog/threat-insight/ta402-uses-complex-ironwind-infection-chains-target-middle-east-based-government>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ironwind>

Last change to this tool card: 17 January 2024

Download this tool card in JSON format

All groups using tool IronWind

Changed	Name	Country	Observed	
APT groups				
	Molerats, Extreme Jackal, Gaza Cybergang	[Gaza]	2012-Jul 2023	

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