Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:08:47 UTC

Tool: Karkoff

Names	Karkoff MailDropper DropperBackdoor CACTUSPIPE OILYFACE
Category	Malware
Type	Backdoor, Dropper
Description	(Talos) In April, Cisco Talos identified an undocumented malware developed in .NET. On the analyzed samples, the malware author left two different internal names in plain text: 'DropperBackdoor' and 'Karkoff.' We decided to use the second name as the malware's moniker, as it is less generic. The malware is lightweight compared to other malware due to its small size and allows remote code execution from the C2 server. There is no obfuscation and the code can be easily disassembled.
Information	<https://blog.talosintelligence.com/2019/04/dnspionage-brings-out-karkoff.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.karkoff>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Karkoff>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool Karkoff

Changed	Name	Country	Observed	
APT groups				
	DNSpionage		2019-Apr 2019	

	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=330eed05-5332-4314-a9ef-ebe891bc3153