Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:37:09 UTC

Tool: Karagany

Names	Karagany Karagny Trojan.Karagany xFrost
Category	Malware
Type	Backdoor, Credential stealer, Downloader, Exfiltration
Description	(SecureWorks) Dating from at least 2010, the Karagany malware family originated from criminal malware known as 'Dream Loader.' Reports indicate that Dream Loader was leaked onto underground forums and that limited use was seen in the wild. Karagany does not have a wealth of built-in capability at its core. Its main purpose is to provide the ability for a remote threat actor to maintain persistent access to a victim's network, upload/download files, and download and execute additional plugin modules. In addition to the plugin functionality, the core module contains a limited capability to harvest browser passwords stored in the Windows Credential Store.
Information	<https://www.secureworks.com/research/updated-karagany-malware-targets-energy-sector>
MITRE ATT&CK	<https://attack.mitre.org/software/S0094/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.karagany>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:karagany>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Karagany

Changed	Name	Country	Observed

APT groups

	Berserk Bear, Dragonfly 2.0		2015-May 2017	
	Energetic Bear, Dragonfly		2010-Mar 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=433ea147-b7bc-458f-95ce-7dbc2d0d7747