Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:58:37 UTC

Tool: Graphiron

Names	Graphiron
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Credential stealer
Description	(Symantec) Graphiron is a two-stage threat consisting of a downloader (Downloader.Graphiron) and a payload (Infostealer.Graphiron). The payload is capable of carrying out the following tasks: • Reads MachineGuid • Obtains the IP address from https://checkip.amazonaws.com • Retrieves the hostname, system info, and user info • Steals data from Firefox and Thunderbird • Steals private keys from MobaXTerm. • Steals SSH known hosts • Steals data from PuTTY • Steals stored passwords • Takes screenshots • Creates a directory • Lists a directory • Runs a shell command • Steals an arbitrary file
Information	<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nodaria-ukraine-infostealer>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.graphiron>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool Graphiron

Changed	Name	Country	Observed	
APT groups				
	SaintBear, Lorec53		2021-Oct 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=6b99018f-62bf-4df9-9a0f-c6209ba5c734