Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:31:22 UTC

Tool: KimJongRAT

Names	KimJongRAT
Category	Malware
Type	Backdoor, Info stealer, Credential stealer, Exfiltration
Description	(Palo Alto) As the original filename “cow_pass.fig” suggests, KimJongRAT seems to be wholly used as a password extraction and information stealer tool by the threat actor, and the collected data are exfiltrated to C2 with support from other malware such as BabyShark or Gh0st RAT. The information that the KimJongRAT malware steals from victim machines include email credentials from Microsoft Outlook and Mozilla Thunderbird, login credentials for Google, Facebook, and Yahoo accounts from browsers Internet Explorer, Chrome, Mozilla Firefox, and Yandex Browser.
Information	<https://unit42.paloaltonetworks.com/babyshark-malware-part-two-attacks-continue-using-kimjongrat-and-pcrat/> <https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/> <https://malware.lu/assets/files/articles/RAP003_KimJongRAT-Stealer_Analysis.1.0.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.kimjongrat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:KimJongRAT>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool KimJongRAT

Changed	Name	Country	Observed
APT groups			

	Kimsuky, Velvet Chollima		2012-Aug 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=1981c06c-cc55-4efe-99e1-ac799d04d3b6