Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:33:49 UTC

Tool: KIVARS

Names	KIVARS
Category	Malware
Type	Reconnaissance
Description	(Trend Micro) The encryption for the initial packets sent by the BKDR_KIVARS uses RC4 as the encryption. It includes the following information: • Victim's IP • Possible Campaign ID • OS version • Hostname • Username • KIVARS version • Recent Document\Desktop folder • Keyboard Layout
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/kivars-with-venom-targeted-attacks-upgrade-with-64-bit-support/> <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt> <https://www.trendmicro.com/en_us/research/17/f/following-trail-blacktech-cyber-espionage-campaigns.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0437/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.kivars>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:kivars>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool KIVARS

Changed	Name	Country	Observed	
APT groups				
	BlackTech, Circuit Panda, Radio Panda		2010-Oct 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=8c076c07-b2f3-4b9e-88b5-638b31d12e2d