Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:41:56 UTC

Tool: JripBot

Names	JripBot Jiripbot
Category	Malware
Type	Reconnaissance, Backdoor, Credential stealer, Info stealer, Loader, Dropper
Description	(Kaspersky) The malware set used by the Wild Neutron threat actor has several component groups, including: • A main backdoor module that initiates the first communication with C&C server • Several information gathering modules • Exploitation tools • SSH-based exfiltration tools • Intermediate loaders and droppers that decrypt and run the payloads Although customized, some of the modules seem to be heavily based on open source tools (e.g. the password dumper resembles the code of Mimikatz and Pass-The-Hash Toolkit) and commercial malware (HTTPS proxy module is practically identical to the one that is used by HesperBot).
Information	<https://securelist.com/wild-neutron-economic-espionage-threat-actor-returns-with-new-tricks/71275/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.jripbot>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Jripbot>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool JripBot

Changed	Name	Country	Observed

APT groups

	Wild Neutron, Butterfly, Sphinx Moth	[Unknown]	2013-Feb 2013	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=742c30fb-2172-4d2a-89db-2112e2bf6971