Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:57:37 UTC

Tool: HiKit

Names	HiKit
Category	Malware
Type	Backdoor, Tunneling
Description	(Novetta) Hikit consists of at least two generations of malware that provides basic RAT functionality. The first generation of Hikit (referred to as “Gen 1”) operates as a server and requires an externally exposed network interface in order for an attacker to access the victim machine. The second generation of Hikit (referred to as “Gen 2”) uses the more traditional client model and beacons out to an attacker’s C2 server. While the communication models shifted dramatically between Gen 1 and Gen 2, both generations of Hikit retain the same basic RAT function consisting of remote command shell, file management, network proxy and port forwarding.
Information	<https://www.novetta.com/wp-content/uploads/2014/11/HiKit.pdf> <https://www.recordedfuture.com/hidden-lynx-analysis/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0009/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.hikit>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:hikit>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool HiKit

Changed	Name	Country	Observed	
APT groups				
	APT 17, Deputy Dog, Elderwood, Sneaky Panda		2009-Jun 2024	

	APT 31, Judgment Panda, Zirconium		2016-Mar 2024	
	Axiom, Group 72		2008-2008/2014	
	Hidden Lynx, Aurora Panda		2009-2014	

4 groups listed (4 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=4b11af2b-ef10-4160-ac62-046b4289e683