Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:38:10 UTC

Tool: Hancitor

Names	Hancitor Chanitor
Category	Malware
Type	Downloader, Loader
Description	(Palo Alto) In the past, Hancitor was sent as a malicious attachment in a spam email which would then download and install the attackers' final malware like a banking Trojan. When they would do this, the Hancitor attachment would download and install the final malware from a malicious or compromised site. But as organizations have gotten more effective at blocking malicious attachments like Hancitor, we've seen the attackers behind Hancitor adapt to evade detection and prevention. They've done this by moving the Hancitor malware from being a malicious attachment in spam to itself being a malicious download. The spam the attackers use no long has a malicious attachment but instead a malicious link that downloads the malicious Hancitor attachment.
Information	<https://unit42.paloaltonetworks.com/threat-brief-hancitor-actors/> <https://unit42.paloaltonetworks.com/hancitor-infections-cobalt-strike/> <https://unit42.paloaltonetworks.com/wireshark-tutorial-hancitor-followup-malware/> <http://www.intel471.com/blog/cobalt-strike-cybercriminals-trickbot-qbot-hancitor> <https://www.binarydefense.com/analysis-of-hancitor-when-boring-begets-beacon/> <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/hancitor-making-use-of-cookies-to-prevent-url-scraping/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0499/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.hancitor>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:hancitor>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Hancitor

Changed	Name	Country	Observed	
Other groups				
	TA511	[Unknown]	2018-Oct 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=75abbd4a-2ff3-4b94-af79-e864af5a4513