Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:20:02 UTC

Other threat group: TA511

Names	TA511 *(Proofpoint)* MAN1 *(?)* Moskalvzapoe *(?)*	
Country	[Unknown]	
Motivation	Financial crime	
First seen	2018	
Description	(Palo Alto) Hancitor is an information stealer and malware downloader used by a threat actor designated as MAN1, Moskalvzapoe or TA511. In a threat brief from 2018, we noted Hancitor was relatively unsophisticated, but it would remain a threat for years to come. Approximately three years later, Hancitor remains a threat and has evolved to use tools like Cobalt Strike. In recent months, this actor began using a network ping tool to help enumerate the Active Directory (AD) environment of infected hosts. This blog illustrates how the threat actor behind Hancitor uses the network ping tool, so security professionals can better identify and block its use.	
Observed	Countries: Argentina, Brazil, Canada, Germany, Hong Kong, India, Ireland, Israel, Italy, Japan, Kazakhstan, Lithuania, Malaysia, Netherlands, Russia, Singapore, South Africa, South Korea, Taiwan, Thailand, Turkey, Ukraine, UK, USA, Vietnam.	
Tools used	Cobalt Strike, Ficker Stealer, Hancitor, NetSupport Manager.	
Operations performed	Oct 2020	Hancitor's Use of Cobalt Strike and a Noisy Network Ping Tool <https://unit42.paloaltonetworks.com/hancitor-infections-cobalt-strike/>
Information	<https://unit42.paloaltonetworks.com/threat-brief-hancitor-actors/>	

Last change to this card: 21 April 2021

Download this actor card in PDF or JSON format