Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:37:11 UTC

Tool: PhantomNet

Names	PhantomNet SManager
Category	Malware
Type	Reconnaissance, Backdoor, Loader
Description	(ESET) The backdoor was named Smanager_ssl.DLL by its developers but we use PhantomNet, as that was the project name used in an older version of this backdoor. This most recent version was compiled on the 26th of April 2020, almost two months before the supply-chain attack. In addition to Vietnam, we have seen victims in the Philippines, but unfortunately we did not uncover the delivery mechanism in those cases. This backdoor is quite simple and most of the malicious capabilities are likely deployed through additional plugins. It can retrieve the victim's proxy configuration and use it to reach out to the command and control (C&C) server. This shows that the targets are likely to be working in a corporate network.
Information	<https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/> <https://insight-jp.nttsecurity.com/post/102glv5/pandas-new-arsenal-part-3-smanager> <https://0xthreatintel.medium.com/reversing-apt-tool-smanager-unpacked-d413a04961c4> <https://0xthreatintel.medium.com/how-to-unpack-smanager-apt-tool-cb5909819214>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.smanager>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool PhantomNet

Changed	Name	Country	Observed
APT groups			

	Operation SignSight	[Unknown]	2020	
	TA428		2013-Jan 2022	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=41b6f923-e7a8-4e88-bbea-1894be386ed4