Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:49:05 UTC

Tool: Nefilim

Names	Nefilim Nephilim
Category	Malware
Type	Ransomware, Big Game Hunting
Description	(Trend Micro) Nefilim is among the notable ransomware variants that use double extortion tactics in their campaigns. First discovered in March 2020, Nefilim threatens to release victims' stolen data to coerce them into paying the ransom. Aside from its use of this tactic, another notable characteristic of Nefilim is its similarity to Nemty; in fact, it is believed to be an evolved version of the older ransomware.
Information	<https://www.trendmicro.com/en_us/research/21/b/nefilim-ransomware.html> <https://www.sisainfosec.com/blogs/nefilim-ransomware/> <https://www.govinfosecurity.com/nephilim-ransomware-gang-tied-to-citrix-gateway-hacks-a-14480> <https://labs.sentinelone.com/meet-nemty-successor-nefilim-nephilim-ransomware/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.nefilim>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:nefilim>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Nefilim

Changed	Name	Country	Observed	
APT groups				
	Traveling Spider	[Unknown]	2019-Mar 2021	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3edfaff6-30ec-4abf-85de-56b4192e6a8c