Traveling Spider - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:58:38 UTC

APT group: Traveling Spider

Names	Traveling Spider *(CrowdStrike)* Gold Mansard *(SecureWorks)*	
Country	[Unknown]	
Motivation	Financial gain	
First seen	2019	
Description	(BleepingComputer) A new ransomware has been spotted over the weekend, carrying references to the Russian president and antivirus software. The researchers call it Nemty. This is the first version of Nemty ransomware, named so after the extension it adds to the files following the encryption process.	
Observed	Countries: Argentina, Algeria, Austria, Belgium, Bhutan, Bolivia, Brazil, Canada, Chile, China, Czech, Denmark, Ecuador, Egypt, Estonia, France, Germany, Ghana, Guatemala, Guinea, Hungary, India, Indonesia, Iran, Italy, Japan, Latvia, Libya, Lithuania, Luxembourg, Malaysia, Morocco, Nepal, Netherlands, Niger, Pakistan, Philippines, Poland, Portugal, Russia, Slovakia, South Africa, South Korea, Spain, Sweden, Thailand, Turkey, UAE, UK, Ukraine, USA, Venezuela, Vietnam.	
Tools used	7-Zip, AdFind, BloodHound, LaZagne, MEGAsync, Mimikatz, Nefilim, Nemty, Network Password Recovery, PsExec, smbtool.	
Operations performed	Sep 2019	Nemty Ransomware Update Lets It Kill Processes and Services <https://www.bleepingcomputer.com/news/security/nemty-ransomware-update-lets-it-kill-processes-and-services/>
	Sep 2019	Fake PayPal Site Spreads Nemty Ransomware <https://www.bleepingcomputer.com/news/security/fake-paypal-site-spreads-nemty-ransomware/>

Sep 2019	Nemty Ransomware Gets Distribution from RIG Exploit Kit <https://www.bleepingcomputer.com/news/security/nemty-ransomware-gets-distribution-from-rig-exploit-kit/>
Oct 2019	Nemty 1.6 Ransomware Released and Pushed via RIG Exploit Kit <https://www.bleepingcomputer.com/news/security/nemty-16-ransomware-released-and-pushed-via-rig-exploit-kit/>
Nov 2019	Nemty Ransomware Expands Its Reach, Also Delivered by Trik Botnet <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nemty-ransomware-trik-botnet>
Jan 2020	Nemty Ransomware to Start Leaking Non-Paying Victim's Data <https://www.bleepingcomputer.com/news/security/nemty-ransomware-to-start-leaking-non-paying-victims-data/>
Feb 2020	Nemty Ransomware Actively Distributed via 'Love Letter' Spam <https://www.bleepingcomputer.com/news/security/nemty-ransomware-actively-distributed-via-love-letter-spam/>
Mar 2020	Nemty Ransomware Punishes Victims by Posting Their Stolen Data <https://www.bleepingcomputer.com/news/security/nemty-ransomware-punishes-victims-by-posting-their-stolen-data/>
Mar 2020	New Nefilim Ransomware Threatens to Release Victims' Data <https://www.bleepingcomputer.com/news/security/new-nefilim-ransomware-threatens-to-release-victims-data/>
Apr 2020	Nemty ransomware operation shuts down public RaaS <https://www.zdnet.com/article/nemty-ransomware-operation-shuts-down/>
May 2020	Toll Group hit by ransomware a second time, deliveries affected <https://www.bleepingcomputer.com/news/security/toll-group-hit-by-ransomware-a-second-time-deliveries-affected/>
May 2020	Beyonce and Victoria's Secret lingerie maker targeted by extortionists <https://news.sky.com/story/beyonce-and-victorias-secret-lingerie-maker-targeted-by-extortionists-11983025>
Jun 2020	Nefilim Hackers Publish Oil Firm Data Online and Continue Disruptive Campaign <https://techmonitor.ai/techonology/cybersecurity/nefilim-hackers-publish-oil-firm>

	Jul 2020	Orange confirms ransomware attack exposing business customers' data <https://www.bleepingcomputer.com/news/security/orange-confirms-ransomware-attack-exposing-business-customers-data/>
	Jul 2020	Business giant Dussmann Group's data leaked after ransomware attack <https://www.bleepingcomputer.com/news/security/business-giant-dussmann-groups-data-leaked-after-ransomware-attack/>
	Nov 2020	Luxottica data breach exposes 820K EyeMed, LensCrafters patients <https://www.bleepingcomputer.com/news/security/luxottica-data-breach-exposes-820k-eyemed-lenscrafters-patients/>
	Dec 2020	Home appliance giant Whirlpool hit in Nefilim ransomware attack <https://www.bleepingcomputer.com/news/security/home-appliance-giant-whirlpool-hit-in-nefilim-ransomware-attack/>
	Jan 2021	Nefilim Ransomware Attack Uses “Ghost” Credentials <https://news.sophos.com/en-us/2021/01/26/nefilim-ransomware-attack-uses-ghost-credentials/>
	Mar 2021	The Nefilim Ransomware Group Has Hit ‘Spirit Airlines’ <https://www.technadu.com/nefilim-ransomware-group-hit-spirit-airlines/252679/>
Information	<https://www.bleepingcomputer.com/news/security/new-nemty-ransomware-may-spread-via-compromised-rdp-connections/>	

Last change to this card: 10 August 2021

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=f0596c9f-822f-4e3c-b2af-fc50630e6ec0