Viking Spider - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Viking Spider

Names	Viking Spider *(CrowdStrike)*
Country	[Unknown]
Motivation	Financial gain
First seen	2019
Description	(Analyst1) Viking Spider first began ransom operations in December 2019, and they use ransomware known as Ragnar Locker to compromise and extort organizations. Below are key findings identified while researching Viking Spider activity. • Viking Spider is the first ransomware attacker to install their own virtual machine (VM) into victim environments. They use this VM to evade detection, and they also use it as a launch point to execute the attack. • The gang is the first to use Facebook ads to pressure victims into paying the ransom. • Viking Spider outsources call centers in India to contact victims asking them to pay the ransom or risk data exposure. • Viking Spider uses Managed Service Provider (MSP) software to deliver malware and hacktools as well as provide remote access into victim environments. • Viking Spider is one of the few gangs who conduct DDoS attacks alongside ransom attacks to pressure victims to pay. Another Cartel gang first used this tactic, but Viking Spider quickly adopted it for their uses as well. • Viking Spider uses social media such as Twitter to shame non-paying victims publicly.
Observed	Sectors: Automotive, Construction, Energy, Hospitality, IT, Law enforcement, Media, Telecommunications. Countries: Greece, Italy, Japan, Portugal, USA.
Tools used	RagnarLocker.

Operations performed	Apr 2020	RagnarLocker ransomware hits EDP energy giant, asks for €10M <https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/>
	May 2020	Ransomware deploys virtual machines to hide itself from antivirus software <https://www.zdnet.com/article/ransomware-deploys-virtual-machines-to-hide-itself-from-antivirus-software/>
	Jul 2020	Ragnar Locker Targets CWT in Ransomware Attack <https://cybelangel.com/blog/ragnar-locker-targets-cwt/>
	Nov 2020	Capcom hit by Ragnar Locker ransomware, 1TB allegedly stolen <https://www.bleepingcomputer.com/news/security/capcom-hit-by-ragnar-locker-ransomware-1tb-allegedly-stolen/>
	Nov 2020	Ransomware Group Turns to Facebook Ads <https://krebsonsecurity.com/2020/11/ransomware-group-turns-to-facebook-ads/>
	Nov 2020	Campari hit by Ragnar Locker Ransomware, $15 million demanded <https://www.bleepingcomputer.com/news/security/campari-hit-by-ragnar-locker-ransomware-15-million-demanded/>
	Jan 2021	Ragnar Locker Ransomware Attack Impacts Employee Records at Dassault Falcon Jet <https://chaslescorp.com/ragnar-locker-ransomware-attack-impacts-employee-records-at-dassault-falcon-jet/>
	Jun 2021	Computer memory maker ADATA hit by Ragnar Locker ransomware <https://www.bleepingcomputer.com/news/security/computer-memory-maker-adata-hit-by-ragnar-locker-ransomware/>
	Sep 2021	Ransomware gang threatens to leak data if victim contacts FBI, police <https://www.bleepingcomputer.com/news/security/ransomware-gang-threatens-to-leak-data-if-victim-contacts-fbi-police/>
	Sep 2021	Customer Care Giant TTEC Hit By Ransomware <https://krebsonsecurity.com/2021/09/customer-care-giant-ttec-hit-by-ransomware/>
	Aug 2022	Ragnar Locker Likely Behind Attack on Greek Gas Operator <https://www.bankinfosecurity.com/ragnar-locker-likely-behind-attack-on-greek-gas-operator-a-19907>
	Sep 2022	Ragnar Locker ransomware claims attack on Portugal's flag airline <https://www.bleepingcomputer.com/news/security/ragnar-locker-

		ransomware-claims-attack-on-portugals-flag-airline/>
	Nov 2022	Ransomware gang targets Belgian municipality, hits police instead <https://www.bleepingcomputer.com/news/security/ransomware-gang-targets-belgian-municipality-hits-police-instead/>
	Aug 2023	Hackers claim to publish prominent Israeli hospital's patient data <https://therecord.media/israel-hospital-data-leaked-ragnar-locker-ransomware>
Counter operations	Oct 2023	Ragnar Locker ransomware's dark web extortion sites seized by police <https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomwares-dark-web-extortion-sites-seized-by-police/>
	Oct 2023	Ragnar Locker ransomware developer arrested in France <https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomware-developer-arrested-in-france/>
Information	<https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf> <https://cybernews.com/security/how-we-applied-to-work-with-ransomware-gang/>	

Last change to this card: 29 November 2023

Download this actor card in PDF or JSON format
