Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:53:09 UTC

Tool: RagnarLocker

Names	RagnarLocker Ragnar Locker
Category	Malware
Type	Ransomware, Big Game Hunting
Description	(McAfee) The RagnarLocker ransomware first appeared in the wild at the end of December 2019 as part of a campaign against compromised networks targeted by its operators. The ransomware code is small (only 48kb after the protection in its custom packer is removed) and coded in a high programming language (C/C++). Like all ransomware, the goal of this malware is to encrypt all files that it can and request a ransom for decrypting them. RagnarLocker's operators, as we have seen with other bad actors recently, threaten to publish the information they get from compromised machines if ransoms are not paid. After conducting reconnaissance, the ransomware operators enter the victim's network and, in some pre-deployment stages, steal information before finally dropping the ransomware that will encrypt all files in the victim's machines. The most notable RagnarLocker attack to date saw this malware deployed in a large company where the malware operators then requested a ransom of close to $11 million USD in return for not leaking information stolen from the company. In this report we will talk about the sample used in this attack.
Information	<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ragnarlocker-ransomware-threatens-to-release-confidential-information/> <https://zawadidone.nl/2020/06/01/lets-analyze-ragnar-locker.html> <https://www.deepinstinct.com/2020/04/27/ragnar-locker-ransomware-unlocked-by-deep-instinct/> <https://resources.infosecinstitute.com/topic/ragnar-locker-malware-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/> <https://securelist.com/targeted-ransomware-encrypting-data/99255/> <https://www.bankinfosecurity.com/fbi-warns-uptick-in-ragnar-locker-ransomware-activity-a-15454>

	<https://www.bleepingcomputer.com/news/security/fbi-ransomware-gang-breached-52-us-critical-infrastructure-orgs/> <https://www.tripwire.com/state-of-security/security-data-protection/ragnar-locker-ransomware-what-you-need-to-know/> <https://www.cybereason.com/blog/threat-analysis-report-ragnar-locker-ransomware-targeting-the-energy-sector>
MITRE ATT&CK	<https://attack.mitre.org/software/S0481/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ragnarlocker>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:ragnarlocker>

Last change to this tool card: 21 April 2025

Download this tool card in JSON format

All groups using tool RagnarLocker

Changed	Name	Country	Observed	
APT groups				
	FIN8	[Unknown]	2016-Dec 2022	
	UNC2447	[Unknown]	2020	
	Viking Spider	[Unknown]	2019-Oct 2023	

3 groups listed (3 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=9a967e7d-f989-4639-97f8-0ab46c34de1c