Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:43:47 UTC

Other threat group: Dungeon Spider

Names	Dungeon Spider *(CrowdStrike)*	
Country	Russia	
Motivation	Financial gain	
First seen	2016	
Description	(CrowdStrike) Dungeon Spider is a criminal group operating the ransomware most commonly known as Locky, which has been active since February 2016 and was last observed in late 2017. Locky is a ransomware tool that encrypts files using a combination of cryptographic algorithms: RSA with a key size of 2,048 bits, and AES with a key size of 128 bits. Locky targets a large number of file extensions and is able to encrypt data on shared network drives. In an attempt to further impact victims and prevent file recovery, Locky deletes all of the Shadow Volume Copies on the machine. Dungeon Spider primarily relies on broad spam campaigns with malicious attachments for distribution. Locky is the community/industry name associated with this actor. Locky has been observed to be distributed via Necurs (operated by Monty Spider).	
Observed	Countries: Worldwide.	
Tools used	Locky.	
Operations performed	Feb 2016	A cyberattack launched against the Hollywood Presbyterian Medical Center has forced staff to declare an “internal emergency” and left employees unable to access patient files. <https://www.zdnet.com/article/hollywood-hospital-becomes-ransomware-victim/>
	Feb 2016	A red marquee bannered on the homepage of the Methodist Hospital in Henderson, Kentucky announced a cyberattack that successfully penetrated their networks, prompting it to operate under an “internal

	state of emergency". <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/locky-ransomware-strain-led-kentucky-hospital-to-an-internal-state-of-emergency>
Apr 2016	Japanese Trends in the Aggressive Activity of the "Locky" Ransomware <https://www.fortinet.com/blog/threat-research/japanese-trends-in-the-aggressive-activity-of-the-locky-ransomware.html>
Jun 2016	Locky Ransomware Hides Under Multiple Obfuscated Layers of JavaScript <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/locky-ransomware-hides-under-multiple-obfuscated-layers-of-javascript/>
Aug 2016	Locky Ransomware Distributed Via DOCM Attachments in Latest Email Campaigns <https://www.fireeye.com/blog/threat-research/2016/08/locky_ransomwaredis.html>
Jan 2017	Without Necurs, Locky Struggles <https://blog.talosintelligence.com/2017/01/locky-struggles.html>
Apr 2017	Now, cybercriminals are using PDFs instead of Word documents to deliver Locky ransomware. <https://www.vadesecure.com/en/locky-malware-comeback/>
Aug 2017	New Locky Ransomware Phishing Attacks Beat Machine Learning Tools <https://www.darkreading.com/attacks-breaches/new-locky-ransomware-phishing-attacks-beat-machine-learning-tools/d/d-id/1330010>
Aug 2017	Locky Ransomware switches to the Lukitus extension for Encrypted Files <https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-the-lukitus-extension-for-encrypted-files/>
Sep 2017	Locky ransomware strikes at Amazon <https://www.pandasecurity.com/mediacenter/malware/locky-ransomware-strikes-amazon/>
Nov 2017	The most recent change for Locky came as one of the most popular ways to spread malware: spear phishing emails. <https://threatvector.cylance.com/en_us/home/threat-spotlight-locky-ransomware.html>

	Feb 2018	Locky Ransomware Is Back in a Big Way <https://shadownet.co.za/2019/07/01/locky-ransomware-is-back-in-a-big-way/>
Information	<https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-october-dungeon-spider/> <https://www.proofpoint.com/us/threat-insight/post/Dridex-Actors-Get-In-the-Ransomware-Game-With-Locky> <https://securelist.com/locky-the-encryptor-taking-the-world-by-storm/74398/> <https://en.wikipedia.org/wiki/Locky>	

Last change to this card: 15 April 2020

Download this actor card in PDF or JSON format
