Doppel Spider - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:45:03 UTC

APT group: Doppel Spider

Names	Doppel Spider *(CrowdStrike)* Gold Heron *(SecureWorks)* Grief Group *(self given)*	
Country	Russia	
Motivation	Financial gain	
First seen	2019	
Description	(CrowdStrike) CrowdStrike Intelligence has identified a new ransomware variant identifying itself as BitPaymer. This new variant was behind a series of ransomware campaigns beginning in June 2019, including attacks against the City of Edcouch, Texas and the Chilean Ministry of Agriculture. We have dubbed this new ransomware DoppelPaymer because it shares most of its code with the BitPaymer ransomware operated by Indrik Spider. However, there are a number of differences between DoppelPaymer and BitPaymer, which may signify that one or more members of Indrik Spider have split from the group and forked the source code of both Dridex and BitPaymer to start their own Big Game Hunting ransomware operation. DoppelPaymer has been observed to be distributed by Smoke Loader (operated by Smoky Spider) and Emotet (operated by Mummy Spider, TA542).	
Observed	Sectors: Government, Manufacturing. Countries: Austria, Brazil, Canada, Chile, Dominican Republic, France, Germany, Greece, Italy, Mexico, Portugal, Spain, Switzerland, Thailand, UK, USA.	
Tools used	Cobalt Strike, DoppelPaymer, Grief.	
Operations performed	Feb 2020	The DoppelPaymer Ransomware is the latest family threatening to sell or publish a victim's stolen files if they do not pay a ransom demand. <https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-sells-victims-data-on-darknet-if-not-paid/>
	Mar 2020	Ransomware scumbags leak Boeing, Lockheed Martin, SpaceX documents after contractor refuses to pay <https://www.theregister.co.uk/2020/04/10/lockheed_martin_spacex_ransomware_leak/>
	Jun 2020	DopplePaymer ransomware gang claims to have breached DMI, a major US IT and cybersecurity provider, and one of NASA IT contractors.

	<https://www.zdnet.com/article/ransomware-gang-says-it-breached-one-of-nasas-it-contractors/>
Aug 2020	UK research university Newcastle University says that it will take several weeks to get IT services back online after DoppelPaymer ransomware operators breached its network and took systems offline on the morning of August 30th. <https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-hits-newcastle-university-leaks-data/>
Sep 2020	Death occurred after a patient was diverted to a nearby hospital after the Duesseldorf University Hospital suffered a ransomware attack. <https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/>
Oct 2020	On October 7th, Hall County in Georgia announced that they had suffered a ransomware attack that impacted their networks and phone systems. <https://www.bleepingcomputer.com/news/security/georgia-county-voter-information-leaked-by-ransomware-gang/>
Nov 2020	Compal, the second-largest laptop manufacturer in the world, hit by ransomware <https://www.zdnet.com/article/compal-the-second-largest-laptop-manufacturer-in-the-world-hit-by-ransomware/>
Nov 2020	MasterChef, Big Brother producer hit by DoppelPaymer ransomware <https://www.bleepingcomputer.com/news/security/masterchef-big-brother-producer-hit-by-doppelpaymer-ransomware/>
Dec 2020	Foxconn electronics giant hit by ransomware, $34 million ransom <https://www.bleepingcomputer.com/news/security/foxconn-electronics-giant-hit-by-ransomware-34-million-ransom/>
Feb 2021	Kia Motors America suffers ransomware attack, $20 million ransom <https://www.bleepingcomputer.com/news/security/kia-motors-america-suffers-ransomware-attack-20-million-ransom/>
Apr 2021	Breach of the Illinois Attorney General's Office <https://illinoisattorneygeneral.gov/pressroom/2021_04/20210413.html>
Jul 2021	DoppelPaymer ransomware gang rebrands as the Grief group <https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-gang-rebrands-as-the-grief-group/>
Sep 2021	Ransomware gang threatens to wipe decryption key if negotiator hired <https://www.bleepingcomputer.com/news/security/ransomware-gang-threatens-to-wipe-decryption-key-if-negotiator-hired/>
Sep 2021	Grief Gang's New Quadruple Extortion Scheme Doesn't Change the Game <https://www.cybereason.com/blog/grief-gangs-new-quadruple-extortion-scheme-doesnt-change-the-game>
Oct 2021	Grief Ransomware Gang Claims 41 New Victims, Targeting Manufacturers; Municipalities; & Service Companies in U.K. & Europe

		<https://www.esentire.com/security-advisories/grief-ransomware-gang-claims-41-new-victims-targeting-manufacturers-municipalities-service-companies-in-u-k-europe>
	Oct 2021	NRA: No comment on Russian ransomware gang attack claims <https://www.bleepingcomputer.com/news/security/nra-no-comment-on-russian-ransomware-gang-attack-claims/>
Counter operations	Feb 2023	Germany and Ukraine hit two high-value ransomware targets <https://www.europol.europa.eu/media-press/newsroom/news/germany-and-ukraine-hit-two-high-value-ransomware-targets>
	Sep 2023	DoppelPaymer ransomware group suspects identified <https://www.malwarebytes.com/blog/news/2023/09/doppelpaymer-ransomware-group-suspects-identified>
	May 2025	Moldova arrests suspect linked to DoppelPaymer ransomware attacks <https://www.bleepingcomputer.com/news/security/moldova-arrests-suspect-linked-to-doppelpaymer-ransomware-attacks/>
Information	<https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/> <https://lifars.com/2019/11/from-dridex-to-bitpaymer-ransomware-to-doppelpaymerthe-evolution/> <https://www.bleepingcomputer.com/news/security/new-doppelpaymer-ransomware-emerges-from-bitpaymers-code/> <https://msrc-blog.microsoft.com/2019/11/20/customer-guidance-for-the-dopplepaymer-ransomware/> <https://beta.documentcloud.org/documents/20428892-doppelpaymer-fbi-pin-on-dec-10-2020>	

Last change to this card: 27 June 2025

Download this actor card in PDF or JSON format
