Indrik Spider - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:13:34 UTC

APT group: Indrik Spider

Names	Indrik Spider *(CrowdStrike)* Gold Drake *(SecureWorks)* Gold Winter *(SecureWorks)* Evil Corp *(self given)* UNC2165 *(Mandiant)* DEV-0243 *(Microsoft)* Manatee Tempest *(Microsoft)* Mustard Tempest *(Microsoft)* Blue Lelantos *(PWC)* G0119 *(MITRE)*
Country	Russia
Motivation	Financial crime, Financial gain
First seen	2007
Description	(CrowdStrike) Indrik Spider is a sophisticated eCrime group that has been operating Dridex since June 2014. In 2015 and 2016, Dridex was one of the most prolific eCrime banking rojans on the market and, since 2014, those efforts are thought to have netted Indrik Spider millions of dollars in criminal profits. Throughout its years of operation, Dridex has received multiple updates with new modules developed and new anti-analysis features added to the malware. In August 2017, a new ransomware variant identified as BitPaymer was reported to have ransomed the U.K.'s National Health Service (NHS), with a high ransom demand of 53 BTC (approximately $200,000 USD). The targeting of an organization rather than individuals, and the high ransom demands, made BitPaymer stand out from other contemporary ransomware at the time. Though the encryption and ransom functionality of BitPaymer was not technically sophisticated, the malware contained multiple anti-analysis features that overlapped with Dridex. Later technical analysis of BitPaymer indicated that it had been developed by Indrik Spider, suggesting the group had expanded its criminal operation to include ransomware as a monetization strategy. Indrik Spider appears to be a subgroup of TA505, Graceful Spider, Gold Evergreen. In 2019, a subgroup of Indrik Spider split off into Doppel Spider.

	Dridex has been observed to be distributed via Necurs (operated by Monty Spider) and Emotet (operated by Mummy Spider, TA542).	
Observed	Sectors: Financial, Government, Healthcare, Media. Countries: Worldwide.	
Tools used	Advanced Port Scanner, Babuk Locker, BitPaymer, Cobalt Strike, Cridex, Dridex, EmpireProject, Hades, Macaw Locker, MEGAsync, Metasploit, Mimikatz, PayloadBIN, Phoenix, PowerSploit, PsExec, Raspberry Robin, SocGholish, WastedLoader, WastedLocker.	
Operations performed	Aug 2017	Several hospitals part of the NHS Lanarkshire board were hit on Friday by a version of the Bit Paymer ransomware. The NHS Lanarkshire board includes hospitals such as Hairmyres Hospital in East Kilbride, Monklands Hospital in Airdrie and Wishaw General Hospital. <https://www.bleepingcomputer.com/news/security/bit-paymer-ransomware-hits-scottish-hospitals/>
	Jul 2018	BitPaymer Ransomware Paralyzes IT Systems of the Alaskan Town <https://socprime.com/en/news/bitpaymer-ransomware-paralyzes-it-systems-of-the-alaskan-town/>
	Jan 2019	Arizona Beverages knocked offline by ransomware attack <https://techcrunch.com/2019/04/02/arizona-beverages-ransomware/>
	May 2019	BitPaymer Ransomware Leveraging New Custom Packer Framework Against Targets Across the U.S. <https://blog.morphisec.com/bitpaymer-ransomware-with-new-custom-packer-framework>
	Aug 2019	Apple Zero-Day Exploited in New BitPaymer Campaign <https://blog.morphisec.com/apple-zero-day-exploited-in-bitpaymer-campaign>
	Oct 2019	Pilz, one of the world's largest producers of automation tools, has been down for more than a week after suffering a ransomware infection. <https://www.zdnet.com/article/major-german-manufacturer-still-down-a-week-after-getting-hit-by-ransomware/>
	Nov 2019	Everis, an NTT DATA company and one of Spain's largest managed service providers (MSP), had its computer systems encrypted today in a ransomware attack, just as it happened to Spain's largest radio station Cadena SER (Sociedad Española de Radiodifusión). <https://www.bleepingcomputer.com/news/security/ransomware-attacks-hit-everis-and-spains-largest-radio-network/>

	May 2020	WastedLocker: A New Ransomware Variant Developed By The Evil Corp Group <https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/>
	Jul 2020	Garmin services and production go down after ransomware attack <https://www.zdnet.com/article/garmin-services-and-production-go-down-after-ransomware-attack/>
	Dec 2020	INDRIK SPIDER Supersedes WastedLocker with Hades Ransomware to Circumvent OFAC Sanctions <https://www.crowdstrike.com/blog/hades-ransomware-successor-to-indrik-spiders-wastedlocker/>
	Mar 2021	Insurance giant CNA hit by new Phoenix CryptoLocker ransomware <https://www.bleepingcomputer.com/news/security/insurance-giant-cna-hit-by-new-phoenix-cryptolocker-ransomware/>
	May 2021	RIG Exploit Kit delivers WastedLoader malware <https://www.bitdefender.com/files/News/CaseStudies/study/397/Bitdefender-PR-Whitepaper-RIG-creat5362-en-EN.pdf>
	Jun 2021	New Evil Corp ransomware mimics PayloadBin gang to evade US sanctions <https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/>
	Sep 2021	Trucking giant Forward Air reports ransomware data breach <https://www.bleepingcomputer.com/news/security/trucking-giant-forward-air-reports-ransomware-data-breach/>
	Oct 2021	Sinclair Broadcast Hack Linked to Notorious Russian Cybergang <https://www.bloomberg.com/news/articles/2021-10-20/sinclair-broadcast-hack-linked-to-notorious-russian-cybergang>
	Oct 2021	Olympus US systems hit by cyberattack over the weekend <https://www.bleepingcomputer.com/news/security/olympus-us-systems-hit-by-cyberattack-over-the-weekend/>
	Dec 2021	Dridex malware trolls employees with fake job termination emails <https://www.bleepingcomputer.com/news/security/dridex-malware-trolls-employees-with-fake-job-termination-emails/>
	Dec 2021	Dridex Omicron phishing taunts with funeral helpline number <https://www.bleepingcomputer.com/news/security/dridex-omicron-phishing-taunts-with-funeral-helpline-number/>
Counter operations	Oct 2015	In the fall of 2015, the Dell SecureWorks Counter Threat Unit (CTU) research team collaborated with the UK National Crime Agency (NCA), the U.S.

		Federal Bureau of Investigation (FBI), and the Shadowserver Foundation to take over the Dridex banking trojan. <https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation>
	Dec 2019	Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in Deployment of “Bugat” Malware <https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens>
	Dec 2019	Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware <https://home.treasury.gov/news/press-releases/sm845>
	Oct 2024	Treasury Sanctions Members of the Russia-Based Cybercriminal Group Evil Corp in Tri-Lateral Action with the United Kingdom and Australia <https://home.treasury.gov/news/press-releases/jy2623>
Information	<https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/> <https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/> <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/spanish-mssp-targeted-by-bitpaymer-ransomware/> <https://www.us-cert.gov/ncas/alerts/aa19-339a> <https://blog.truesec.com/2021/05/05/are-the-notorious-cyber-criminals-evil-corp-actually-russian-spies/> <https://www.secureworks.com/research/threat-profiles/gold-winter> <https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0119/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
