Pinchy Spider, Gold Southfield - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Pinchy Spider, Gold Southfield

Names	Pinchy Spider *(CrowdStrike)* Gold Southfield *(SecureWorks)* Gold Garden *(SecureWorks)* G0115 *(MITRE)*	
Country	Russia	
Motivation	Financial gain	
First seen	2018	
Description	(CrowdStrike) CrowdStrike Intelligence has recently observed Pinchy Spider affiliates deploying GandCrab ransomware in enterprise environments, using lateral movement techniques and tooling commonly associated w nation-state adversary groups and penetration testing teams. This change in tactics makes Pinchy Spider and its affiliates the latest eCrime adversaries to join the growing trend of targeted, low-volume/high-return ransomwa deployments known as “big game hunting.” Pinchy Spider is the criminal group behind the development of the ransomware most commonly known as Gan which has been active since January 2018. Pinchy Spider sells access to use GandCrab ransomware under a par program with a limited number of accounts. The program is operated with a 60-40 split in profits (60 percent to customer), as is common among eCrime actors, but Pinchy Spider is also willing to negotiate up to a 70-30 spli “sophisticated” customers. GandCrab and Sodinokibi have been observed to be distributed by DanaBot (operated by Scully Spider, TA547 Taurus Loader (operated by Venom Spider, Golden Chickens).	
Observed	Countries: Worldwide.	
Tools used	certutil, Cobalt Strike, GandCrab, Sodinokibi, VIDAR.	
Operations performed	Apr 2019	Sodinokibi ransomware exploits WebLogic Server vulnerability <https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html>
	Jun 2019	Yesterday night, a source in the malware community has told ZDNet that the GandCrab RaaS ope formally announced plans to shut down their service within a month. The announcement was made in an official thread on a well-known hacking forum, where the Ga RaaS has advertised its service since January 2018, when it formally launched. <https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/>
	Aug 2019	Over 20 Texas local governments hit in 'coordinated ransomware attack' <https://www.zdnet.com/article/at-least-20-texas-local-governments-hit-in-coordinated-ransomwa attack/>
	Dec 2019	CyrusOne, one of the biggest data center providers in the US, has suffered a ransomware attack, Z has learned. <https://www.zdnet.com/article/ransomware-attack-hits-major-us-data-center-provider/>

Dec 2019	Sodinokibi Ransomware Behind Travelex Fiasco: Report <https://threatpost.com/sodinokibi-ransomware-travelex-fiasco/151600/>
Dec 2019	A crypto virus that attacked the Albany County Airport Authority's computer management provid during the Christmas holiday period ended up infecting the authority's servers as well, encrypting and demanding a ransom payment. <https://www.timesunion.com/business/article/Ransomware-attack-cripples-airport-authority-s-14963401.php>
Jan 2020	New Jersey Synagogue Suffers Sodinokibi Ransomware Attack <https://www.bleepingcomputer.com/news/security/new-jersey-synagogue-suffers-sodinokibi-ransomware-attack/>
Jan 2020	Sodinokibi Ransomware Publishes Stolen Data for the First Time They claim this data belongs to Artech Information Systems, who describe themselves as a 'minor women-owned diversity supplier and one of the largest IT staffing companies in the U.S', and that will release more if a ransom is not paid. <https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-publishes-stolen-data the-first-time/>
Feb 2020	The operators of the Sodinokibi Ransomware (REvil) have started urging affiliates to copy their v data before encrypting computers so it can be used as leverage on a new data leak site that is bein launched soon. <https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-may-tip-nasdaq-on-a to-hurt-stock-prices/>
Feb 2020	The operators behind Sodinokibi Ransomware published download links to files containing what claim is financial and work documents, as well as customers' personal data stolen from giant U.S. house Kenneth Cole Productions. <https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-posts-alleged-data-of kenneth-cole-fashion-giant/>
Mar 2020	The operators of the Sodinokibi Ransomware are threatening to publicly share a company's 'dirty' financial secrets because they refused to pay the demanded ransom. As organizations decide to restore their data manually or via backups instead of paying ransoms, ransomware operators are escalating their attacks. <https://www.bleepingcomputer.com/news/security/ransomware-threatens-to-reveal-companys-di secrets/>
Mar 2020	Recently, the Sodinokibi Ransomware operators published over 12 GB of stolen data allegedly be to a company named Brooks International for not paying the ransom. <https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-data-leaks-now-sold-hacker-forums/>
Apr 2020	Sodinokibi Ransomware to stop taking Bitcoin to hide money trail <https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-to-stop-taking-bitcoi hide-money-trail/>
Apr 2020	SeaChange video platform allegedly hit by Sodinokibi ransomware <https://www.bleepingcomputer.com/news/security/seachange-video-platform-allegedly-hit-by-sodinokibi-ransomware/>
May 2020	REvil ransomware threatens to leak A-list celebrities' legal docs <https://www.bleepingcomputer.com/news/security/revil-ransomware-threatens-to-leak-a-list-cele legal-docs/>

May 2020	REvil ransomware gang publishes 'Elexon staff's passports' after UK electrical middleman shrugs attack <https://www.theregister.com/2020/06/01/elexon_ransomware_was_revil_sodinokibi/>
May 2020	Here come REvil ransomware operators with another massive data leak. In this instance, they leal confidential data of Agromart Group, well-known crop production partners. <https://cybleinc.com/2020/06/02/times-up-for-agromart-group-and-their-data-got-leaked-by-revi ransomware-operators/>
Jun 2020	REvil ransomware creates eBay-like auction site for stolen data <https://www.bleepingcomputer.com/news/security/revil-ransomware-creates-ebay-like-auction-s stolen-data/>
Jun 2020	REvil ransomware operators have been observed while scanning one of their victim's network for of Sale (PoS) servers by researchers with Symantec's Threat Intelligence team. <https://www.bleepingcomputer.com/news/security/revil-ransomware-scans-victims-network-for- of-sale-systems/>
Jun 2020	The threat actor behind the Sodinokibi (REvil) ransomware is demanding a $14 million ransom fr Brazilian-based electrical energy company Light S.A. <https://www.securityweek.com/ransomware-operators-demand-14-million-power-company>
Jul 2020	A ransomware gang has infected the internal network of Telecom Argentina, one of the country's l internet service providers, and is now asking for a $7.5 million ransom demand to unlock encrypt <https://www.zdnet.com/article/ransomware-gang-demands-7-5-million-from-argentinian-isp/>
Jul 2020	Administrador de Infraestructuras Ferroviarias (ADIF), a Spanish state-owned railway infrastruct manager was hit by REVil ransomware operators. <https://securityaffairs.co/wordpress/106304/cyber-crime/adif-revil-ransomware-attack.html>
Aug 2020	Brown-Forman, one of the largest U.S. companies in the spirits and wine business, suffered a cyb attack. The intruders allegedly copied 1TB of confidential data. <https://www.bleepingcomputer.com/news/security/us-spirits-and-wine-giant-hit-by-cyberattack- data-stolen/>
Sep 2020	REvil ransomware deposits $1 million in hacker recruitment drive <https://www.bleepingcomputer.com/news/security/revil-ransomware-deposits-1-million-in-hack recruitment-drive/>
Oct 2020	REvil ransomware gang claims over $100 million profit in a year <https://www.bleepingcomputer.com/news/security/revil-ransomware-gang-claims-over-100-mill profit-in-a-year/>
Oct 2020	Today, the threat actors added GPI (Gaming Partners International) to their dedicated leak site. GI describes itself as a leading provider of casino currency and table game equipment worldwide. <https://www.databreaches.net/revil-ransomware-threat-actors-reveal-their-gaming-company-vict
Nov 2020	Flagship Group revealed last night that its systems were compromised by a 'cyberattack' on Sunda November. <https://www.theregister.com/2020/11/06/revil_sodinokibi_ransomware_gang_flagship_group_h
Nov 2020	REvil ransomware gang 'acquires' KPOT malware <https://www.zdnet.com/article/revil-ransomware-gang-acquires-kpot-malware/>
Nov 2020	Managed web hosting provider Managed.com has taken their servers and web hosting systems of they struggle to recover from a weekend REvil ransomware attack. <https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-managedcom-hosting- provider-500k-ransom/>

Jan 2021	Pan-Asian retail giant Dairy Farm suffers REvil ransomware attack <https://www.bleepingcomputer.com/news/security/pan-asian-retail-giant-dairy-farm-suffers-revi ransomware-attack/>
Mar 2021	Ransomware gang plans to call victim's business partners about attacks <https://www.bleepingcomputer.com/news/security/ransomware-gang-plans-to-call-victims-busir partners-about-attacks/>
Mar 2021	Computer giant Acer hit by $50 million ransomware attack <https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ranso attack/>
Mar 2021	REvil ransomware has a new ‘Windows Safe Mode’ encryption mode <https://www.bleepingcomputer.com/news/security/revil-ransomware-has-a-new-windows-safe-n encryption-mode/>
Mar 2021	REvil ransomware can now reboot infected devices <https://www.bankinfosecurity.com/revil-ransomware-now-reboot-infected-devices-a-16259>
Apr 2021	Asteelflash electronics maker hit by REvil ransomware attack <https://www.bleepingcomputer.com/news/security/asteelflash-electronics-maker-hit-by-revil- ransomware-attack/>
Apr 2021	REvil ransomware now changes password to auto-login in Safe Mode <https://www.bleepingcomputer.com/news/security/revil-ransomware-now-changes-password-to- login-in-safe-mode/>
Apr 2021	Leading cosmetics group Pierre Fabre hit with $25 million ransomware attack <https://www.bleepingcomputer.com/news/security/leading-cosmetics-group-pierre-fabre-hit-witl million-ransomware-attack/>
Apr 2021	REvil gang tries to extort Apple, threatens to sell stolen blueprints <https://www.bleepingcomputer.com/news/security/revil-gang-tries-to-extort-apple-threatens-to-s stolen-blueprints/>
Apr 2021	Brazil's Rio Grande do Sul court system hit by REvil ransomware <https://www.bleepingcomputer.com/news/security/brazils-rio-grande-do-sul-court-system-hit-by ransomware/>
May 2021	FBI: JBS ransomware attack was carried out by REvil <https://therecord.media/fbi-jbs-ransomware-attack-was-carried-out-by-revil/>
Jun 2021	Fujifilm confirms ransomware attack disrupted business operations <https://www.bleepingcomputer.com/news/security/fujifilm-confirms-ransomware-attack-disrupt business-operations/>
Jun 2021	US nuclear weapons contractor Sol Oriens has suffered a cyberattack allegedly at the hands of the ransomware gang, which claims to be auctioning data stolen during the attack. <https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-us-nuclear-weapons- contractor/>
Jun 2021	Relentless REvil, revealed: RaaS as variable as the criminals who use it <https://news.sophos.com/en-us/2021/06/11/relentless-revil-revealed/>
Jun 2021	Healthcare giant Grupo Fleury hit by REvil ransomware attack <https://www.bleepingcomputer.com/news/security/healthcare-giant-grupo-fleury-hit-by-revil- ransomware-attack/>

	Jun 2021	Fashion titan French Connection says 'FCUK' as REvil-linked ransomware makes off with data <https://www.theregister.com/2021/06/24/french_connection_says_fcuk_as/>
	Jul 2021	Spanish telecom giant MasMovil hit by Revil ransomware gang <https://www.hackread.com/revil-ransomware-gang-hits-masmovil-telecom/>
	Jul 2021	Kaseya hijacked, thousands attacked by REvil, fix delayed again <https://blog.malwarebytes.com/cybercrime/2021/07/shutdown-kaseya-vsa-servers-now-amidst-cascading-revil-attack-against-msps-clients/>
	Jul 2021	REvil ransomware gang's web sites mysteriously shut down <https://www.bleepingcomputer.com/news/security/revil-ransomware-gangs-web-sites-mysteriou shut-down/>
	Sep 2021	UK VoIP telco receives 'colossal ransom demand', reveals REvil cybercrooks suspected of 'organi DDoS attacks on UK VoIP companies <https://www.theregister.com/2021/09/02/uk_voip_telcos_revil_ransom/>
	Sep 2021	REvil ransomware group returns following Kaseya attack <https://therecord.media/revil-ransomware-group-returns-following-kaseya-attack/>
	Sep 2021	REvil ransomware is back in full attack mode and leaking data <https://www.bleepingcomputer.com/news/security/revil-ransomware-is-back-in-full-attack-mod leaking-data/>
	Sep 2021	REvil ransomware devs added a backdoor to cheat affiliates <https://www.bleepingcomputer.com/news/security/revil-ransomware-devs-added-a-backdoor-to-affiliates/>
	Oct 2021	Hong Kong marketing firm Fimmick has been hit with a ransomware attack, according to a Britis cybersecurity firm monitoring the situation. <https://www.zdnet.com/article/hong-kong-firm-becomes-latest-marketing-company-hit-with-rev ransomware/>
	Jan 2022	After Russian Arrests, REvil Implants Persist <https://blog.reversinglabs.com/blog/after-russian-arrests-revil-rolls-on>
	Apr 2022	REvil's TOR sites come alive to redirect to new ransomware operation <https://www.bleepingcomputer.com/news/security/revils-tor-sites-come-alive-to-redirect-to-new ransomware-operation/>
	May 2022	REvil ransomware returns: New malware sample confirms gang is back <https://www.bleepingcomputer.com/news/security/revil-ransomware-returns-new-malware-samp confirms-gang-is-back/>
	May 2022	REvil Resurgence? Or a Copycat? <https://www.akamai.com/blog/security/revil-resurgence-or-copycat>
Counter operations	Jul 2020	GandCrab ransomware operator arrested in Belarus <https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-operator-arrested-in-b
	Mar 2021	GandCrab ransomware distributor arrested in South Korea <https://therecord.media/gandcrab-ransomware-distributor-arrested-in-south-korea/>
	Sep 2021	REvil Affiliates Confirm: Leadership Were Cheating Dirtbags <https://threatpost.com/revil-affiliates-leadership-cheated-ransom-payments/174972/>
	Oct 2021	REvil ransomware shuts down again after Tor sites were hijacked <https://www.bleepingcomputer.com/news/security/revil-ransomware-shuts-down-again-after-tor were-hijacked/>

		<https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil pushing-it-offline-2021-10-21/>
	Oct 2021	Two ransomware operators arrested in Ukraine <https://therecord.media/two-ransomware-operators-arrested-in-ukraine/>
	Oct 2021	German investigators identify REvil ransomware gang core member <https://www.bleepingcomputer.com/news/security/german-investigators-identify-revil-ransomw gang-core-member/>
	Nov 2021	REvil ransomware affiliates arrested in Romania and Kuwait <https://www.bleepingcomputer.com/news/security/revil-ransomware-affiliates-arrested-in-romar kuwait/>
	Nov 2021	US seizes $6 million from REvil ransomware, arrest Kaseya hacker <https://www.bleepingcomputer.com/news/security/us-seizes-6-million-from-revil-ransomware-a kaseya-hacker/>
	Nov 2021	Five affiliates to Sodinokibi/REvil unplugged <https://www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged>
	Nov 2021	U.S. offers $10 million reward for leaders of REvil ransomware <https://www.bleepingcomputer.com/news/security/us-offers-10-million-reward-for-leaders-of-re ransomware/>
	Nov 2021	FBI seized $2.3M from affiliate of REvil, Gandcrab ransomware gangs <https://www.bleepingcomputer.com/news/security/fbi-seized-23m-from-affiliate-of-revil-gandcr ransomware-gangs/>
	Jan 2022	Russia arrests REvil ransomware gang members, seize $6.6 million <https://www.bleepingcomputer.com/news/security/russia-arrests-revil-ransomware-gang-membe seize-66-million/>
	May 2024	Sodinokibi/REvil Affiliate Sentenced for Role in $700M Ransomware Scheme <https://www.justice.gov/opa/pr/sodinokibirevil-affiliate-sentenced-role-700m-ransomware-scher
	Oct 2024	Russia sentences REvil ransomware members to over 4 years in prison <https://www.bleepingcomputer.com/news/security/russia-sentences-revil-ransomware-members- 4-years-in-prison/>
Information		<https://www.crowdstrike.com/blog/pinchy-spider-adopts-big-game-hunting/> <https://krebsonsecurity.com/2019/07/whos-behind-the-gandcrab-ransomware/> <https://www.secureworks.com/blog/revil-the-gandcrab-connection> <https://blog.morphisec.com/threat-profile-gandcrab-ransomware> <https://www.kpn.com/security-blogs/Tracking-REvil.htm> <https://www.cybereason.com/blog/the-sodinokibi-ransomware-attack> <https://securityintelligence.com/posts/sodinokibi-revil-ransomware-disrupt-trade-secrets/> <https://threatpost.com/revil-spill-details-us-attacks/166669/> <https://news.sophos.com/en-us/2021/06/11/relentless-revil-revealed/> <https://unit42.paloaltonetworks.com/revil-threat-actors/> <https://www.bankinfosecurity.com/revils-cybercrime-reputation-in-tatters-will-reboot-a-17802> <https://therecord.media/how-a-texas-hack-changed-the-ransomware-business-forever/> <https://www.darkreading.com/cyberattacks-data-breaches/revil-actor-russia-planning-2021-kaseya-attack>
MITRE ATT&CK		<https://attack.mitre.org/groups/G0115/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
