Wizard Spider, Gold Blackburn - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:43:21 UTC

APT group: Wizard Spider, Gold Blackburn

Names	Wizard Spider *(CrowdStrike)* Grim Spider *(CrowdStrike)* TEMP.MixMaster *(FireEye)* Gold Blackburn *(SecureWorks)* Gold Ulrick *(SecureWorks)* ITG23 *(IBM)* DEV-0193 *(Microsoft)* Storm-0230 *(Microsoft)* Periwinkle Tempest *(Microsoft)* G0102 *(MITRE)*
Country	Russia
Motivation	Financial crime, Financial gain
First seen	2014
Description	Wizard Spider is reportedly associated with Lunar Spider. (Crowdstrike) The Wizard Spider threat group is the Russia-based operator of the TrickBot banking malware. This represents a growing criminal enterprise of which Grim Spider appears to be a subset. The Lunar Spider threat gro Eastern European-based operator and developer of the commodity banking malware called BokBot (aka IcedID), first observed in April 2017. The BokBot malware provides Lunar Spider affiliates with a variety of capabilities to credential theft and wire fraud, through the use of webinjects and a malware distribution function. Dyre has been observed to be distributed by Cutwail (operated by Narwhal Spider), as well as their own botnets G Upatre. TrickBot has been observed to be distributed via Emotet (operated by Mummy Spider, TA542), BokBot (operated Spider), Smoke Loader (operated by Smoky Spider), DanaBot (operated by Scully Spider, TA547), Kelihos (opera Zombie Spider), Necurs (operated by Monty Spider) and Taurus Loader (operated by Venom Spider, Golden Chic well as their own botnet Gophe.
Observed	Sectors: Defense, Financial, Government, Healthcare, Telecommunications. Countries: Worldwide.
Tools used	AdFind, Anchor, BazarBackdoor, BloodHound, Cobalt Strike, Conti, Diavol, Dyre, Gophe, Invoke-SMBAutoBru LaZagne, LightBot, PowerSploit, PowerTrick, PsExec, Ryuk, SessionGopher, TrickBot, TrickMo, Upatre.
Operations performed	Apr 2019: Cybercriminals Spoof Major Accounting and Payroll Firms in Tax Season Malware Campaigns <https://securityintelligence.com/cybercriminals-spoof-major-accounting-and-payroll-firms-in-tax-s malware-campaigns/> Jun 2019: During June and July, F5 researchers first noticed Trickbot campaigns aimed at a smaller set of geog oriented targets and did not use redirection attacks—a divergence from previous Trickbot characteri <https://www.f5.com/labs/articles/threat-intelligence/tricky-trickbot-runs-campaigns-without-redire

Aug 2019	In a recent analysis in our cybercrime research labs, we noticed changes in the deployment of the Tr Trojan. At the time, the change we observed only applied to infection attempts on Windows 10 64-b operating systems (OSs). In those cases, TrickBot ran the payload, but did not save its typical modul configurations to disk. <https://securityintelligence.com/posts/the-curious-case-of-a-fileless-trickbot-infection/>
Oct 2019	Computers at the DCH Regional Medical Center in Tuscaloosa, Fayette Medical Center and Northp Medical Center were infected with ransomware. <https://www.bbc.com/news/technology-49905226>
Oct 2019	Shipping giant Pitney Bowes hit by ransomware <https://techcrunch.com/2019/10/14/pitney-bowes-ransomware-attack/>
Nov 2019	Louisiana was hit by Ryuk, triggering another cyber-emergency <https://arstechnica.com/information-technology/2019/11/louisiana-was-hit-by-ryuk-triggering-ano emergency/>
Dec 2019	TrickBot Widens Infection Campaigns in Japan Ahead of Holiday Season <https://securityintelligence.com/posts/trickbot-widens-infection-campaigns-in-japan-ahead-of-holi season/>
Dec 2019	The Deadly Planeswalker: How The TrickBot Group United High-Tech Crimeware & APT <https://labs.sentinelone.com/the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-cri apt/>
Dec 2019	The cyberattack that took down public-access computers at Volusia County, Fla., libraries last montl ransomware that has elicited millions of dollars in ransom payments from governments and large bu <https://www.govtech.com/security/Ryuk-Ransomware-behind-Attack-on-Florida-Library-System.h
Dec 2019	New Orleans latest apparent victim of Ryuk ransomware <https://statescoop.com/new-orleans-latest-apparent-victim-of-ryuk-ransomware/>
Dec 2019	An infection with the Ryuk ransomware took down a maritime facility for more than 30 hours; the U Guard said in a security bulletin it published before Christmas. <https://www.zdnet.com/article/us-coast-guard-discloses-ryuk-ransomware-infection-at-maritime-fa
Dec 2019	Suspected Ryuk ransomware attack locks down Adelaide's City of Onkaparinga council <https://www.abc.net.au/news/2020-01-06/city-of-onkaparinga-hit-by-ryuk-ransomware/11843598>
Jan 2020	On the heels of a Ryuk ransomware attack on the Tampa Bay Times, researchers reported a new vari Ryuk stealer being aimed at government, financial and law enforcement targets. <https://www.scmagazine.com/home/security-news/tampa-bay-times-hit-by-ryuk-new-variant-of-st aimed-at-govt-finance/>
Jan 2020	Electronic Warfare Associates (EWA), a 40-year-old electronics company and a well-known US gov contractor, has suffered a ransomware infection, ZDNet has learned. <https://www.zdnet.com/article/dod-contractor-suffers-ransomware-infection/>
Jan 2020	Top-Tier Russian Organized Cybercrime Group Unveils Fileless Stealthy “PowerTrick” Backdoor f Value Targets <https://labs.sentinelone.com/top-tier-russian-organized-cybercrime-group-unveils-fileless-stealthy- powertrick-backdoor-for-high-value-targets/>
Feb 2020	Ryuk Ransomware Campaign Targets Port Lavaca City Hall <https://www.cisomag.com/ryuk-ransomware-campaign-targets-port-lavaca-city-hall/>
Feb 2020	EMCOR Group, a US-based Fortune 500 company specialized in engineering and industrial constru services, disclosed last month a ransomware incident that took down some of its IT systems. <https://www.zdnet.com/article/ryuk-ransomware-hits-fortune-500-company-emcor/>

Feb 2020	Epiq Global, an international e-discovery and managed services company, has taken its systems offl globally after detecting unauthorized activity. <https://www.lawsitesblog.com/2020/03/epiq-global-down-as-company-investigates-unauthorized-a on-systems.html>
Mar 2020	Trickbot campaign targets Coronavirus fears in Italy <https://news.sophos.com/en-us/2020/03/04/trickbot-campaign-targets-coronavirus-fears-in-italy/>
Mar 2020	EVRAZ, one of the world's largest steel manufacturers and mining operations, has been hit by ransc source inside the company told ZDNet today. <https://www.zdnet.com/article/one-of-roman-abramovichs-companies-got-hit-by-ransomware/>
Mar 2020	The City of Durham, North Carolina has shut down its network after suffering a cyberattack by the I Ransomware this weekend. <https://www.bleepingcomputer.com/news/security/ryuk-ransomware-behind-durham-north-carolin cyberattack/>
Mar 2020	New Variant of TrickBot Being Spread by Word Document <https://www.fortinet.com/blog/threat-research/new-variant-of-trickbot-being-spread-by-word-document.html>
Mar 2020	New TrickBot Module Bruteforces RDP Connections, Targets Select Telecommunication Services i Hong Kong <https://labs.bitdefender.com/2020/03/new-trickbot-module-bruteforces-rdp-connections-targets-sel telecommunication-services-in-us-and-hong-kong/>
Mar 2020	TrickBot Pushing a 2FA Bypass App to Bank Customers in Germany <https://securityintelligence.com/posts/trickbot-pushing-a-2fa-bypass-app-to-bank-customers-in-ger
Apr 2020	BazarBackdoor: TrickBot gang's new stealthy network-hacking malware <https://www.bleepingcomputer.com/news/security/bazarbackdoor-trickbot-gang-s-new-stealthy-ne hacking-malware/>
Apr 2020	TrickBot Campaigns Targeting Users via Department of Labor FMLA Spam <https://securityintelligence.com/posts/trickbot-campaigns-targeting-users-via-department-of-labor-spam/>
Apr 2020	As early as April 2020, TrickBot updated one of its propagation modules known as "mworm" to a n module called "nworm." Infections caused through nworm leave no artifacts on an infected DC, and disappear after a reboot or shutdown. <https://unit42.paloaltonetworks.com/goodbye-mworm-hello-nworm-trickbot-updates-propagation-
Jul 2020	Collaboration between FIN7 and the RYUK group <https://blog.truesec.com/2020/12/22/collaboration-between-fin7-and-the-ryuk-group-a-truesec-investigation/>
Jul 2020	The infamous TrickBot trojan has started to check the screen resolutions of victims to detect whethe malware is running in a virtual machine. <https://www.bleepingcomputer.com/news/security/trickbot-malware-now-checks-screen-resolution analysis/>
Jul 2020	Leading toy maker Mattel hit by ransomware <https://www.bleepingcomputer.com/news/security/leading-toy-maker-mattel-hit-by-ransomware/>
Aug 2020	University of Utah pays $457,000 to ransomware gang <https://www.zdnet.com/article/university-of-utah-pays-457000-to-ransomware-gang/>
Aug 2020	Conti (Ryuk) joins the ranks of ransomware gangs operating data leak sites <https://www.zdnet.com/article/conti-ryuk-joins-the-ranks-of-ransomware-gangs-operating-data-lea

Sep 2020	US Court Hit by “Conti” Ransomware <https://www.cbronline.com/news/conti-ransomware-court>
Sep 2020	Universal Health Services (UHS), a Fortune 500 hospital and healthcare services provider, has repo down systems at healthcare facilities around the US after a cyber-attack that hit its network during e Sunday morning. <https://www.bleepingcomputer.com/news/security/uhs-hospitals-hit-by-reported-country-wide-ryu ransomware-attack/>
Oct 2020	French IT giant Sopra Steria hit by Ryuk ransomware <https://www.bleepingcomputer.com/news/security/french-it-giant-sopra-steria-hit-by-ryuk-ransom
Oct 2020	Steelcase furniture giant hit by Ryuk ransomware attack <https://www.bleepingcomputer.com/news/security/steelcase-furniture-giant-hit-by-ryuk-ransomwa
Nov 2020	LightBot: TrickBot’s new reconnaissance malware for high-value targets <https://www.bleepingcomputer.com/news/security/lightbot-trickbot-s-new-reconnaissance-malwar value-targets/>
Nov 2020	Online education giant K12 Inc. has paid a ransom after their systems were hit by Ryuk ransomware middle of November. <https://www.bleepingcomputer.com/news/security/k12-online-schooling-giant-pays-ryuk-ransomw stop-data-leak/>
Jan 2021	FatFace sends controversial data breach email after ransomware attack <https://www.bleepingcomputer.com/news/security/fatface-sends-controversial-data-breach-email-a ransomware-attack/>
Jan 2021	Scottish Environment Protection Agency refuses to pay ransomware crooks over 1.2GB of stolen da <https://www.theregister.com/2021/01/18/scottish_environment_protection_agency_refuses_to_pay
Feb 2021	Trickbot Rebirths Emotet: 140,000 Victims in 149 Countries in 10 Months <https://blog.checkpoint.com/2021/12/08/trickbot-rebirths-emotet-140000-victims-in-149-countries months/>
Mar 2021	Ryuk ransomware hits 700 Spanish government labor agency offices <https://www.bleepingcomputer.com/news/security/ryuk-ransomware-hits-700-spanish-government agency-offices/>
Mar 2021	Ransomware gang wanted $40 million in Florida schools cyberattack <https://www.bleepingcomputer.com/news/security/ransomware-gang-wanted-40-million-in-florida cyberattack/>
Apr 2021	BazarLoader deploys a pair of novel spam vectors <https://news.sophos.com/en-us/2021/04/15/bazarloader/>
May 2021	Green Energy Company Volue Hit by Ransomware <https://www.securityweek.com/green-energy-company-volue-hit-ransomware>
May 2021	Conti ransomware also targeted Ireland's Department of Health <https://www.bleepingcomputer.com/news/security/conti-ransomware-also-targeted-irelands-depart health/>
May 2021	Ireland’s Health Services hit with $20 million ransomware demand <https://www.bleepingcomputer.com/news/security/ireland-s-health-services-hit-with-20-million-ransomware-demand/> <https://www.bleepingcomputer.com/news/security/conti-ransomware-gives-hse-ireland-free-decryp selling-data/>
May 2021	New Zealand hospitals infected by ransomware, cancel some surgeries <https://www.theregister.com/2021/05/19/new_zealand_hospitals_taken_down/>

May 2021	Operation “BazaFlix” The threat actor created a robust fake movie streaming service called BravoMovies, complete with f titles as a landing page. <https://www.proofpoint.com/us/blog/threat-insight/bazaflix-bazaloader-fakes-movie-streaming-ser
May 2021	Exagrid pays $2.6m to Conti ransomware attackers <https://www.computerweekly.com/news/252501665/Exagrid-pays-26m-to-Conti-ransomware-attac
Jun 2021	City of Liege, Belgium hit by ransomware <https://therecord.media/city-of-liege-belgium-hit-by-ransomware/>
Jun 2021	Tulsa warns of data breach after Conti ransomware leaks police citations <https://www.bleepingcomputer.com/news/security/tulsa-warns-of-data-breach-after-conti-ransomw police-citations/>
Jun 2021	Diavol - A New Ransomware Used By Wizard Spider? <https://www.fortinet.com/blog/threat-research/diavol-new-ransomware-used-by-wizard-spider>
Aug 2021	Conti ransomware prioritizes revenue and cyberinsurance data theft <https://www.bleepingcomputer.com/news/security/conti-ransomware-prioritizes-revenue-and-cyberinsurance-data-theft/>
Aug 2021	Nokia subsidiary discloses data breach after Conti ransomware attack <https://www.bleepingcomputer.com/news/security/nokia-subsidiary-discloses-data-breach-after-co ransomware-attack/>
Sep 2021	JVCKenwood hit by Conti ransomware claiming theft of 1.5TB data <https://www.bleepingcomputer.com/news/security/jvckenwood-hit-by-conti-ransomware-claiming 15tb-data/>
Oct 2021	Conti gang threatens to dump victim data if ransom negotiations leak to reporters <https://therecord.media/conti-gang-threatens-to-dump-victim-data-if-ransom-negotiations-leak-to-
Oct 2021	Sandhills online machinery markets shut down by ransomware attack <https://www.bleepingcomputer.com/news/security/sandhills-online-machinery-markets-shut-down ransomware-attack/>
Oct 2021	Conti Ransom Gang Starts Selling Access to Victims <https://krebsonsecurity.com/2021/10/conti-ransom-gang-starts-selling-access-to-victims/>
Nov 2021	Celebrity jewelry house Graff falls victim to ransomware <https://blog.malwarebytes.com/ransomware/2021/11/celebrity-jewelry-house-graff-falls-victim-to- ransomware/>
Nov 2021	Data breach impacts 80,000 South Australian govt employees [Frontier Software] <https://www.bleepingcomputer.com/news/security/data-breach-impacts-80-000-south-australian-g employees/>
Nov 2021	From Shathak Emails to the Conti Ransomware <https://www.cybereason.com/blog/threat-analysis-report-from-shatak-emails-to-the-conti-ransomw <https://www.bleepingcomputer.com/news/security/trickbot-teams-up-with-shatak-phishers-for-con ransomware-attacks/>
Dec 2021	Nordic Choice Hotels hit by Conti ransomware, no ransom demand yet <https://www.bleepingcomputer.com/news/security/nordic-choice-hotels-hit-by-conti-ransomware- ransom-demand-yet/>
Dec 2021	Conti and Karma actors attack healthcare provider at same time through ProxyShell exploits <https://news.sophos.com/en-us/2022/02/28/conti-and-karma-actors-attack-healthcare-provider-at-s through-proxyshell-exploits/>

Dec 2021	Australian Electricity Provider 'CS Energy' Hit by Ransomware <https://www.securityweek.com/australian-electricity-provider-cs-energy-hit-ransomware>
Dec 2021	McMenamins breweries hit by a Conti ransomware attack <https://www.bleepingcomputer.com/news/security/mcmenamins-breweries-hit-by-a-conti-ransomw attack/>
Dec 2021	Shutterfly services disrupted by Conti ransomware attack <https://www.bleepingcomputer.com/news/security/shutterfly-services-disrupted-by-conti-ransomw attack/>
Dec 2021	RR Donnelly has confirmed that threat actors stole data in a December cyberattack, confirmed by BleepingComputer to be a Conti ransomware attack. <https://www.bleepingcomputer.com/news/security/marketing-giant-rrd-confirms-data-theft-in-cont ransomware-attack/>
Dec 2021	Indonesia's central bank confirms ransomware attack, Conti leaks data <https://www.bleepingcomputer.com/news/security/indonesias-central-bank-confirms-ransomware- conti-leaks-data/>
Jan 2022	The Conti ransomware gang has been linked to an attack on Delta Electronics, a Taiwanese electron manufacturing company and a major supplier of power components to companies like Apple and Te <https://therecord.media/conti-ransomware-hits-apple-tesla-supplier/>
Jan 2022	KP Snacks giant hit by Conti ransomware, deliveries disrupted <https://www.bleepingcomputer.com/news/security/kp-snacks-giant-hit-by-conti-ransomware-deliv disrupted/>
Feb 2022	A Modern Ninja: Evasive Trickbot Attacks Customers of 60 High-Profile Companies <https://research.checkpoint.com/2022/a-modern-ninja-evasive-trickbot-attacks-customers-of-60-hi companies/>
Feb 2022	The TrickBot Saga’s Finale Has Aired: Spinoff is Already in the Works <https://www.advintel.io/post/the-trickbot-saga-s-finale-has-aired-but-a-spinoff-is-already-in-the-w
Feb 2022	Something strange is going on with Trickbot <https://intel471.com/blog/trickbot-2022-emotet-bazar-loader>
Feb 2022	Trickbot Group’s AnchorDNS Backdoor Upgrades to AnchorMail <https://securityintelligence.com/posts/new-malware-trickbot-anchordns-backdoor-upgrades-ancho
Feb 2022	Panasonic: February ransomware attack only affected Canada branch <https://therecord.media/panasonic-february-ransomware-attack-only-affected-canada-branch/>
Mar 2022	Ransomware gang Conti has already bounced back from damage caused by chat leaks, experts say <https://www.cyberscoop.com/ransomware-gang-conti-bounced-back/>
Mar 2022	Shutterfly discloses data breach after Conti ransomware attack <https://www.bleepingcomputer.com/news/security/shutterfly-discloses-data-breach-after-conti-rans attack/>
Mar 2022	Ransomware Gang Leaks Files Stolen From Industrial Giant Parker Hannifin <https://www.securityweek.com/ransomware-gang-leaks-files-stolen-industrial-giant-parker-hannifi
Mar 2022	Snap-on discloses data breach claimed by Conti ransomware gang <https://www.bleepingcomputer.com/news/security/snap-on-discloses-data-breach-claimed-by-cont ransomware-gang/>
Apr 2022	The Parker-Hannifin Corporation announced a data breach exposing employees' personal informatic Conti ransomware gang began publishing allegedly stolen data last month.

		<https://www.bleepingcomputer.com/news/security/engineering-firm-parker-discloses-data-breach-a ransomware-attack/>
	Apr 2022	Wind turbine firm Nordex hit by Conti ransomware attack <https://www.bleepingcomputer.com/news/security/wind-turbine-firm-nordex-hit-by-conti-ransomw attack/>
	Apr 2022	Conti ransomware attack was aimed at destabilizing government transition, Costa Rican president sa <https://therecord.media/conti-ransomware-attack-was-aimed-at-destabilizing-government-transitio rican-president-says/> <https://therecord.media/ransomware-gang-threatens-to-overthrow-new-costa-rica-government-rais demand-to-20-million/> <https://therecord.media/son-of-conti/>
	Apr 2022	Unprecedented Shift: The Trickbot Group is Systematically Attacking Ukraine <https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine/>
	May 2022	Conti ransomware claims to have hacked Peru MOF – Dirección General de Inteligencia (DIGIMIN <https://securityaffairs.co/wordpress/131093/cyber-crime/conti-ransomware-peru-direccion-general inteligencia.html>
	Jun 2022	Conti ransomware group's pulse stops, but did it fake its own death? <https://blog.malwarebytes.com/ransomware/2022/06/conti-ransomware-disappears-did-it-fake-its-d death/>
Counter operations	Nov 2015	Russia's FSB quietly led an operation to take down the world's most active cybercriminal groups, th operators of the banking malware Dyre <https://www.forbes.com/sites/thomasbrewster/2016/02/08/russia-arrests-dyre-malware-masterminc
	Sep 2020	In recent weeks, the U.S. military has mounted an operation to temporarily disrupt what is describec world's largest botnet — one used also to drop ransomware, which officials say is one of the top thr 2020 election. <https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/1 0a32-11eb-a166-dc429b380d10_story.html>
	Oct 2020	We disrupted Trickbot through a court order we obtained as well as technical action we executed in partnership with telecommunications providers around the world. We have now cut off key infrastru those operating Trickbot will no longer be able to initiate new infections or activate ransomware alre dropped into computer systems. <https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-election
	Jun 2021	Latvian National Charged for Alleged Role in Transnational Cybercrime Organization <https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-org
	Aug 2021	Disgruntled ransomware affiliate leaks the Conti gang's technical manuals <https://therecord.media/disgruntled-ransomware-affiliate-leaks-the-conti-gangs-technical-manuals/
	Sep 2021	TrickBot gang member arrested after getting stuck in South Korea due to COVID-19 pandemic <https://therecord.media/trickbot-gang-member-arrested-after-getting-stuck-in-south-korea-due-to-c pandemic/>
	Sep 2021	Irish police seize Conti domains used in HSE ransomware attack <https://www.itpro.co.uk/security/ransomware/360786/irish-police-seize-conti-domains-used-in-hse ransomware-attack>
	Oct 2021	TrickBot malware dev extradited to U.S. faces 60 years in prison <https://www.bleepingcomputer.com/news/security/trickbot-malware-dev-extradited-to-us-faces-60 prison/>
	Feb 2022	Conti ransomware gang chats leaked by pro-Ukraine member <https://therecord.media/conti-ransomware-gang-chats-leaked-by-pro-ukraine-member/>

		<https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/> <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/> <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/> <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iv-cryptocrime/>
	Mar 2022	Exposing initial access broker with ties to Conti <https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/>
	Mar 2022	More Conti ransomware source code leaked on Twitter out of revenge <https://www.bleepingcomputer.com/news/security/more-conti-ransomware-source-code-leaked-on out-of-revenge/>
	May 2022	Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice <https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspi justice/>
	Feb 2023	Russian man pleads guilty to laundering Ryuk ransomware money <https://www.bleepingcomputer.com/news/security/russian-man-pleads-guilty-to-laundering-ryuk-ransomware-money/>
	Sep 2023	United States and United Kingdom Sanction Additional Members of the Russia-Based Trickbot Cyb Gang <https://home.treasury.gov/news/press-releases/jy1714>
	Dec 2023	TrickBot malware dev pleads guilty, faces 35 years in prison <https://www.bleepingcomputer.com/news/security/trickbot-malware-dev-pleads-guilty-faces-35-ye prison/> <https://www.bleepingcomputer.com/news/security/russian-trickbot-malware-dev-sentenced-to-64-r prison/>
	May 2025	Germany doxxes Conti ransomware and TrickBot ring leader <https://www.bleepingcomputer.com/news/security/germany-doxxes-conti-ransomware-and-trickbo leader/>
Information		<https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/> <https://www.crowdstrike.com/blog/wizard-spider-lunar-spider-shared-proxy-module/> <https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/> <https://www.crowdstrike.com/blog/wizard-spider-adversary-update/> <https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html> <https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/> <https://www.prodaft.com/m/reports/Conti_TLPWHITE_v1.6_WVcSEtc.pdf> <https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships> <https://www.secureworks.com/blog/gold-ulrick-continues-conti-operations-despite-public-disclosures> <https://www.prodaft.com/m/reports/WizardSpider_TLPWHITE_v.1.4.pdf> <https://www.group-ib.com/media/conti-armada-report/> <https://intel471.com/blog/conti-break-up-contileaks-july-2022> <https://flashpoint.io/blog/history-of-conti-ransomware/> <https://www.deepinstinct.com/blog/an-inside-look-at-the-conti-group>
MITRE ATT&CK		<https://attack.mitre.org/groups/G0102/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format