WIZARD SPIDER

[/ˈwɪz.ərd ˈspaɪ.dər/]

WIZARD SPIDER is a Russian-speaking cybercriminal group active since 2016, best known for operating TrickBot, Ryuk, and Conti-related ransomware. It poses a critical global threat due to financially motivated ransomware and data extortion campaigns targeting major industries worldwide.

IDENTITY

Attribution	: Russian-speaking cybercriminal syndicate assessed to operate primarily from Russia or CIS countries. Believed to have affiliations with Conti and Ryuk ransomware operations.
Active Since	: ~2016
Aliases	: GOLD BLACKBURN, DEV-0193, DEV-0237, Pistachio Tempest, Storm-0193, FIN12, UNC2053.
Motivation	: Financial gain through large-scale ransomware operations, credential theft, and corporate extortion.

TTPs

Initial Access	: Phishing emails with malicious attachments, exploitation of VPN and RDP vulnerabilities, and use of stolen credentials obtained through infostealer malware (e.g., TrickBot, Emotet, IcedID).
Persistence	: Deployment of backdoors such as TrickBot and Cobalt Strike; creation of domain accounts for long-term access.
Command & Control (C2)	: Utilizes encrypted HTTPS, SOCKS proxies, and Cobalt Strike beacons; known to pivot via compromised network infrastructure.
Tools & Malware	: TrickBot, Ryuk, Conti, BazarLoader, Cobalt Strike, AnchorDNS, and Black Basta ransomware. Transitioned from TrickBot to BazarLoader and AnchorMail post-2022.
Techniques	: Double extortion (data encryption + data leak), lateral movement using PsExec and RDP, privilege escalation via Mimikatz, and exfiltration using Rclone or Mega.

TARGET PROFILE

Target Sectors	: Healthcare, Manufacturing, Finance, Retail, and Logistics.
Geographies Targeted	: Global — major campaigns across North America, Europe, and Asia-Pacific with a strong focus on U.S.-based critical infrastructure and enterprises.

THREAT ASSESSMENT

Risk Level	: Critical (Global Impact)
Most Recent Activity	: 2024–2025 campaigns linked to Black Basta and Royal ransomware variants, leveraging phishing and supply chain intrusions against critical infrastructure.
Evolution	: Transitioned from Ryuk/Conti lineage to newer ransomware families (e.g., Black Basta, Quantum). Increased collaboration with other eCrime affiliates and deployment of modular intrusion frameworks integrating infostealers and loaders.

NOTABLE OPERATIONS

- **2018 – Ryuk Ransomware Wave:** Attacked U.S. hospitals and municipal networks causing major disruptions.
- **2020 – Conti Expansion:** Shifted to a Ransomware-as-a-Service model, focusing on high-value enterprise targets.
- **2022 – TrickBot Takedown Resilience:** Continued operations using BazarLoader and AnchorMail after law enforcement takedowns.
- **2023 – Black Basta Emergence:** Rebranded operations under Black Basta, focusing on double extortion and corporate data leaks.
- **2025 – Global Healthcare Attacks:** Coordinated ransomware campaign against hospitals and pharmaceutical manufacturers using hybrid TrickBot–Black Basta infrastructure.