ZEROFOX INTELLIGENCE

Flash

Threat Collective Conducting In-Person Data Theft

F-2026-06-01a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Physical Security, Ransomware, Threat Actor

June 1, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 7:00 AM (EDT) on June 1, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Threat Collective Conducting In-Person Data Theft

| Key Findings

- On May 26, 2026, the Federal Bureau of Investigation (FBI) issued a report highlighting that the ransomware and digital extortion (R&DE) collective Silent Ransom Group (SRG) is conducting physical security breaches against victim infrastructure, in addition to routine social engineering techniques such as phishing emails or phone calls.
- This is the first observed example of an R&DE collective that has visited a target organization in person to gain physical access to its systems. It demonstrates an added threat that will likely inspire other R&DE collectives.
- In December 2024, ZeroFox identified a leak site called "LeakedData" (hosted at hXXp://business-data-leaks[.]com), which is almost certainly SRG's official leak site, given the victims listed on this site majorly overlap with the entities targeted in SRG's recent in-person data theft campaign.
- Although physical intrusion operations require greater resources and carry higher operational risks than traditional cyberattacks, the success of such campaigns is likely to form a blueprint for other R&DE operations against high-value targets.

Details

On May 26, 2026, the FBI issued a report highlighting that R&DE collective SRG is conducting physical security breaches against victim infrastructure, in addition to routine social engineering techniques such as phishing emails or phone calls.[1] If remote access is not acquired, SRG reportedly sends an individual in person to the target organization in order to gain physical access to its systems such as phishing emails or phone calls.

- SRG is a financially motivated R&DE threat collective that has been active since at least 2022 and has conducted data theft and extortion attacks without typically using traditional ransomware encryption.

Historically, SRG has posed as IT support through phone calls and phishing emails to gain access to target infrastructure and exfiltrate data (typically through remote access tools). However, if this fails, SRG reportedly visits the victim organization in person to conduct a physical intrusion and exfiltrate data to an external hard drive or USB drive attached to target infrastructure.

- Notably, this is the first observed example of an R&DE collective that has visited a target organization in person to gain physical access to its systems. It demonstrates an added threat that will likely inspire other R&DE collectives.

Since 2022, SRG has been attributed to data theft and extortion campaigns majorly targeting financial services and legal consulting firms in North America. SRG is likely a remnant or offshoot of the now-defunct Conti ransomware collective due to similarities in some of their tactics, techniques, and procedures (TTPs).

- In December 2023, an FBI Private Industry Notification mentioned SRG's callback phishing method (also known as BazaCall or BazarCall method) as its intrusion vector in several extortion attacks targeting U.S. entities.[2]
- The BazarBackdoor malware deployed in these campaigns was a tool originally developed by the Trickbot collective, which was acquired by Conti in early 2022.

[1] hXXps://www.ic3[.]gov/CSA/2026/260526.pdf
[2] hXXps://www.ic3[.]gov/CSA/2023/231108.pdf

Conti eventually dissolved in mid-2022 due to internal conflicts regarding geopolitical stances on the Russian invasion of Ukraine.[3]

- Conti's dissolution resulted in creation of subgroups, of which SRG is very likely one.

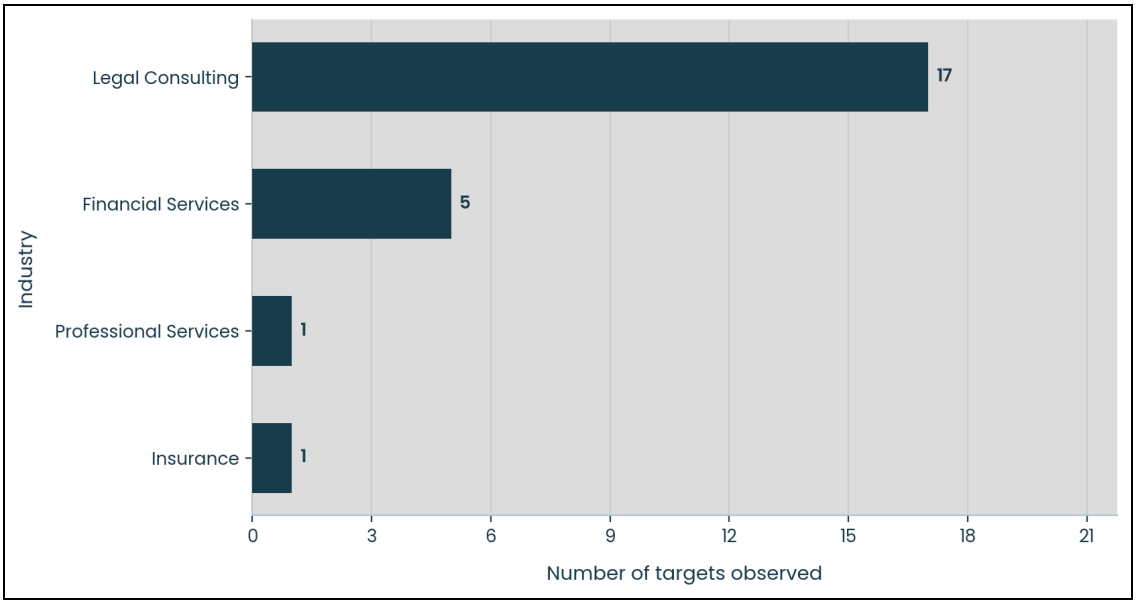
In December 2024, ZeroFox identified a leak site called LeakedData (hosted at hXXp://business-data-leaks[.]com), which is almost certainly SRG's official leak site, given the victims listed on this site majorly overlap with the entities targeted in SRG's recent in-person data theft campaign.

- The three most recent targets listed on the site, as of May 20, 2026, are U.S.-based law firms Orrick, Herrington & Sutcliffe LLP; Jones Day; and Wood Smith Henning & Berman LLP, which have all been targeted by SRG.[4][5]
- Of the victims listed on the site between January and May 2026, about 90 percent are from the legal and consulting industry, with all of them located in the U.S.-Canada region.

[3] hXXps://thehackernews[.]com/2022/10/bazarcall-callback-phishing-attacks.html

[4] hXXps://databreaches[.]net/2026/04/10/silent-ransom-group-leaked-another-big-law-firm-orrick-herrington-sutcliffe/

[5] hXXps://www.abajournal[.]com/news/article/jones-day-latest-big-law-firm-to-fall-victim-to-cyber-phishing-incident



Targeted industries, as listed on LeakedData (2026)

Source: ZeroFox Intelligence

SRG's historical ties to Conti-linked tooling and tradecraft indicate that the group is likely drawing from established cybercriminal methods while adapting them to changing defensive environments. There is a roughly even chance that the group will further evolve its phishing strategies and use artificial intelligence (AI) to produce more believable lures to reflect the changing cybersecurity landscape.

SRG's use of physical access operations, which is not usually part of common extortion campaigns, is likely intended to bypass evolving digital safety protocols against typical cyber intrusion techniques, such as unauthorized remote access. While the tactic may be particularly effective against organizations that store large volumes of confidential information, there is currently insufficient evidence to assess whether it is intended exclusively for the legal sector.

- Even though social engineering and callback phishing remain effective intrusion vectors, physically accessing victim infrastructure likely enables threat actors to bypass certain technical safeguards and directly exfiltrate sensitive data when remote access attempts fail.

Although physical intrusion operations require greater resources and carry higher operational risks than traditional cyberattacks, the success of such campaigns is likely to form a blueprint for other R&DE operations against high-value targets. Moreover, this likely increases the possibility of insider threats, wherein threat actors such as SRG hire existing employees of a target company or send recruits as new hires to infiltrate the company's network.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** **TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** **TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** **TLP:AMBER+STRICT** restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** **TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** **TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** **TLP:CLEAR** information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%