FBI FLASH
ACTIONABLE CYBER INTELLIGENCE
26 MAY 2026
FLASH Number
FLASH-20260526-01

Silent Ransom Group Impersonating IT Personnel through Social Engineering

Summary

The Silent Ransom Group (SRG), also known as Luna Moth, Chatty Spider, and UNC3753, is targeting law firms using social engineering techniques. Through phone calls and phishing emails, SRG actors pose as IT support to establish access to victim computers and exfiltrate data, usually through legitimate remote access tools or by sending an individual in-person to the victim company's location to gain physical access to computers. While SRG has victimized companies in many sectors including those in the insurance, finance, and healthcare industries, the group has consistently targeted US-based law firms since Spring 2023.

Threat

SRG actors—active since at least 2022—conduct data theft and extortion operations without relying on traditional ransomware encryption. Unlike conventional ransomware actors, SRG actors typically seek rapid access to victim systems, immediate data exfiltration, and extortion through threats of public disclosure or sale of stolen data.

Historically, SRG actors sent phishing emails purportedly to charge small "subscription fees" to gain access to victim networks. To cancel the fake subscription, the victim was instructed to call the threat actor, who then emailed the victim a link to download remote access software.

As of Spring 2026, SRG actors use a social engineering scheme to pose as an employee from the victim's IT department. SRG actors either directly call or send phishing emails to urge employees to call the SRG actor posing as IT support. While on the phone, the SRG actor directs the employee to grant access to a remote desktop session. If that attempt fails, SRG sends a threat actor to the victim's location to gain access to insert a storage device into the victim's computer. In this scheme, the threat actor tells the victim they need to image the device or create a backup file to address potential impacts from the phishing email.

Once the threat actor obtains access to the victim's device, they minimally escalate privileges and quickly pivot to data exfiltration without encryption. SRG actors use WinSCP (Windows Secure Copy) or a hidden or renamed version of "Rclone" to exfiltrate data. SRG actors also exfiltrate data to internal filesharing platforms such as Google Drive or Microsoft OneDrive. By sending someone in-person to the victim's location to facilitate the intrusion, SRG actors exfiltrate data to an external hard drive or USB drive inserted

by the threat actor into the victim's computer. SRG actors use the exfiltrated victim data to extort the victim by sending a ransom email threatening to sell or post the data online. SRG actors also call employees or clients of a victim company to pressure the victim to begin ransom negotiations. SRG actors have a public-facing website, business-data-leaks[.]com, where they post victim data.

MITRE ATT&CK Mapping

ATT&CK Tactic	Technique	Relevance to SRG Activity
Initial Access	T1566 – Phishing	Callback phishing emails using invoice, billing, subscription, or IT-themed lures
Resource Development / Social Engineering	T1598.004 – Voice Phishing	Threat actors direct victims to initiate phone contact or impersonate internal IT support
Execution	T1219 – Remote Access Software	Legitimate remote administration tools used to establish interactive access
Credential Access	T1078 – Valid Accounts	Threat actors may leverage victim credentials to access email or cloud services
Collection	T1560 – Archive Collected Data	Data may be staged or compressed prior to exfiltration
Collection	T1530 – Data from Cloud Storage	Theft of data from Microsoft 365, OneDrive, Google Drive, or similar platforms
Exfiltration	T1567 – Exfiltration Over Web Service	Upload of stolen data to cloud storage or web-accessible platforms
Exfiltration	T1052.001 – Exfiltration to Removable Media	In-person intrusion scenarios involving USB or external hard drive data theft
Impact	T1657 – Financial Theft / Extortion	Threatened publication or sale of stolen victim data

Indicators

Recent SRG campaigns left few artifacts on compromised machines. Traditional antivirus products are also unlikely to flag the intrusion because SRG generally uses legitimate system management or remote access tools to carry out the attack. Use of these tools should not be attributed as malicious without analytical evidence to support they are used at the direction of, or controlled by, SRG actors.

Indicators of an SRG attack may include the following:

- New, unauthorized downloads of system management or remote access tools, including Zoho Assist, Quick Assist, AnyDesk, RustDesk, Syncro, Splashtop, or Atera.
- Unauthorized installation of external hard drives or USB drives on company computers.
- Exfiltration of data to Microsoft OneDrive, Google Drive, or external servers.

- WinSCP or Rclone connection made to an external IP address.
- Alerts that data was exfiltrated from the company environment.
- Unidentified or unauthorized individuals attempting to access computers and claiming to be IT support.
- Emails, phone calls, or voicemails from an unnamed group claiming data was stolen.
- Emails or phone calls to clients claiming that their data was stolen.
- Employees receiving unsolicited phone calls from individuals falsely claiming to work in their IT department.

Information Requested

The FBI is seeking any information from SRG victims that can be legally shared, including:

- A copy of the ransom note.
- The phone number or email account used by the threat actor.
- Transcripts of communications with the threat actor, to include voicemails.
- The original call back message or phishing email.
- Cryptocurrency wallet information.
- Special sensitivities of stolen data.
- Identifying information of individuals posing as IT support, including surveillance videos and any photos provided.

Your organization has no obligation to respond or provide information back to the FBI in response to this product. If, after reviewing the information provided, your organization decides to provide information to the FBI, reporting must be consistent with applicable state and federal laws.

Recommendations

Implementing and practicing basic cyber hygiene to include using robust passwords, multifactor authentication, and installation of antivirus tools can possibly defend against ransomware attacks. The FBI recommends the following actions to defend against SRG threat actors:

- Verify the credentials of all individuals accessing company spaces, including obtaining copies of each visitor's ID card.
- Limit access to sensitive data from less secure networks, such as home or public internet.
- Develop and communicate policies regarding when and how IT support will communicate and authenticate themselves to employees.
- Conduct staff training on identifying, resisting, and reporting phishing attempts.

- Maintain regular backups of company data.
- Require phishing-resistant multi-factor authentication (MFA) for as many services as possible.
- If possible, block access to port 22, which enables encrypted remote access, file transfers, and secure command execution on network devices.
- If possible, disable remote access and external drive installation permissions on company computers with access to sensitive or confidential data.

Reporting Notice

If you identify suspicious activity within your enterprise or have information related to the contents of this document, please contact your local FBI Cyber Squad immediately at **www.fbi.gov/contact-us/field-offices**. The FBI also encourages you to report suspicious or criminal activity to the FBI Internet Crime Complaint Center at **www.ic3.gov**. When available, each report should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Individual indicators included in this document should always be evaluated in light of your complete information security situation. Some indicators, particularly those of a nondeterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise.

Administrative Note

The information in this document is being provided by the FBI "as is" for informational purposes only, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cybersecurity professionals and system administrators guard against the persistent malicious actions of cyber actors. The FBI does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the FBI.

This FLASH was coordinated with DHS/CISA and is marked **TLP:CLEAR**. The information in this product may be shared without restriction. Information is subject to standard copyright rules.