Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

23 May 2025

PIN Number

20250523-001

The following information is being provided by the FBI, 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 cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS/CISA.

This PIN has been released **TLP:CLEAR**

Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.

www.fbi.gov/contact-us/field-offices

Silent Ransom Group Targeting Law Firms

Summary

The cyber threat actor Silent Ransom Group (SRG), also known as Luna Moth, Chatty Spider, and UNC3753, is targeting law firms using information technology (IT) themed social engineering calls, and callback phishing emails, to gain remote access to systems or devices and steal sensitive data to extort the victims. While SRG has historically victimized companies in many sectors, starting Spring 2023, the group has consistently targeted US-based law firms, likely due to the highly sensitive nature of legal industry data.

**SRG targets other sectors as well, to include companies in the medical industry and insurance industry. However, most of SRG's victims are law firms or companies with similar naming conventions*.

Threat

SRG has been operating since 2022 and has primarily been known for their callback phishing emails, masquerading as well-known businesses who offer subscription plans. Typically, SRG phishing emails purport to charge small amounts of "subscription fees" as they are less likely to

generate immediate suspicion. In order to cancel the fake subscription, the victim is instructed to call the threat actor who emails a link which downloads remote access software giving the actor access to their device or system. Once the actor has established persistent access, the threat actors will seek to identify valuable information to exfiltrate, before sending a ransom notice to the victim threatening to share the victim's data if a ransom is not paid.

As of March 2025, SRG was observed changing their tactics to calling individuals and posing as an employee from their company's IT department. SRG will then direct the employee to join a remote access session, either through an email sent to them, or navigating to a web page. Once the employee grants access to their device, they are told that work needs to be done overnight.

Once in the victim's device, a typical SRG attack involves minimal privilege escalation and quickly pivots to data exfiltration conducted through "WinSCP" (Windows Secure Copy) or a hidden or renamed version of "Rclone." If the compromised device does not have administrative privileges, WinSCP portable is used to exfiltrate victim data. Although this tactic has only been observed recently, it has been highly effective and resulted in multiple compromises.

Similar to their phishing emails posing as a company with a subscription, once SRG exfiltrates data, they extort the victim by sending them a ransom email threatening to sell or post the data online. SRG will also call employees at a victim company to pressure them into engaging in ransom negotiations. SRG has developed a publicly available site to post victim data, however, they are inconsistent in their use of the site, and do not always follow through on posting victim data.

Indicators

Recent SRG campaigns leave few artifacts on compromised machines. They are also unlikely to be flagged by traditional antivirus products because SRG generally uses legitimate system management or remote access tools to carry out the attacks. Network defenders are therefore advised to treat the following as potential, but not definitive, indications of SRG activity:

- New unauthorized downloads of system management or remote access tools, including Zoho Assist, Syncro, AnyDesk, Splashtop, or Atera.
- WinSCP or Rclone connection made to an external IP address.
- Emails from an unnamed group claiming data was stolen.
- Voicemails or phone calls from an unnamed group claiming data was stolen.
- Emails regarding subscription services providing a phone number and requiring a call to remove pending renewal charges.
- Employees receiving unsolicited phone calls from individuals claiming to work in their IT department.

Recommendations

Implement basic cyber hygiene to include being suspicious, robust passwords, multifactor authentication, and installation of antivirus tools. For SRG threat actors:

- Conduct staff training on resisting phishing attempts
- Develop and communicate policies surrounding when and how company's IT will authenticate themselves with employees
- Maintain regular backups of company data
- Implement two-factor authentication for all employees

Information Requested

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

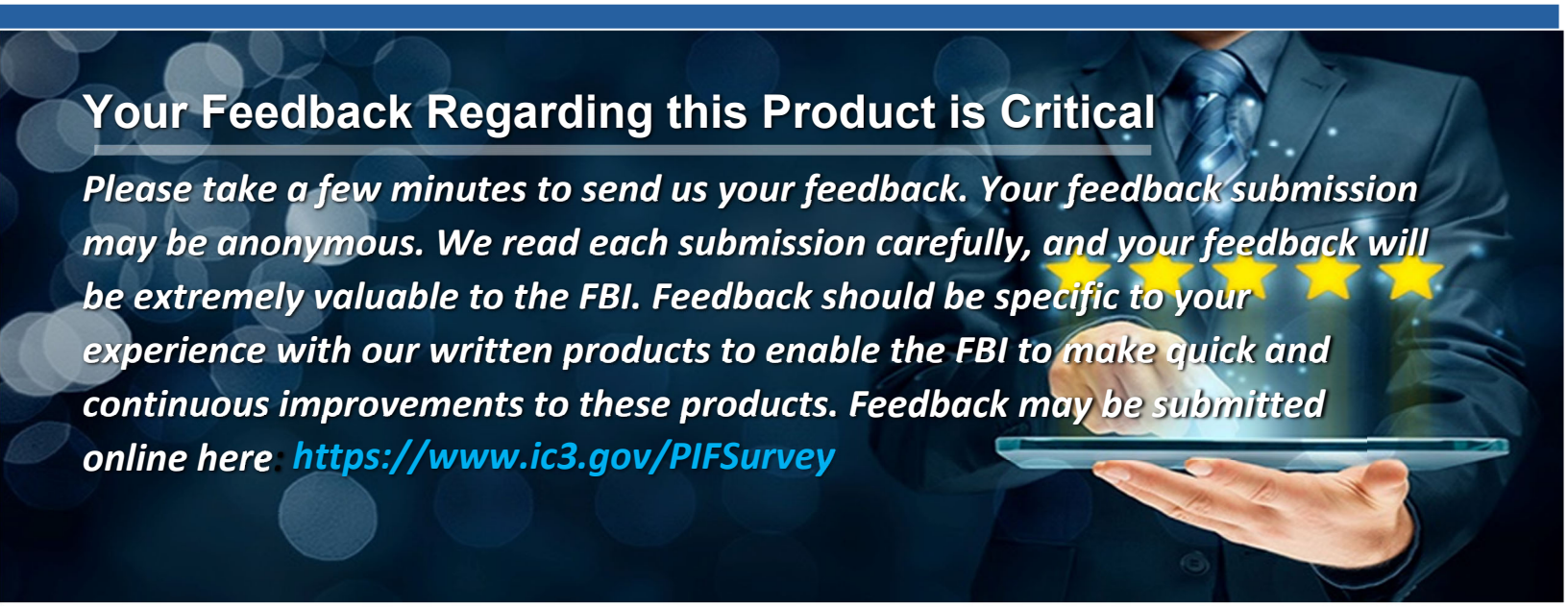
- Ransom Note copy
- Phone number used by Threat Actor
- Communications with Threat Actor to include voicemails
- Cryptocurrency wallet information
- Special sensitivities of stolen data
- Original call back message or phishing email

Your organization has no obligation to respond or provide information back to 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.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted 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.

Administrative Note

The information in this report is being provided “as is” for informational purposes only. 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 product is marked TLP:CLEAR. Subject to standard copyright rules, the information in this product may be shared without restriction.