



THREAT INTELLIGENCE REPORT · OCTOBER 2026

Inside the Luna Moth Files: Reconstructing Silent Ransom Group's Operating Model

An analysis of a newly exposed archive attributed to Silent Ransom Group (Luna Moth, UNC3753), and what it suggests about how the group organizes social-engineering-led extortion.

Table of Contents

01 Executive Summary	1
02 Introduction	2
03 The Luna Moth Files	3
04 What the Exposure Reveals	5
05 Reconstructed Operating Workflow	9
06 Conclusions	10
About Check Point Exposure Management	11

CHAPTER 01

Executive Summary

An anonymous onion site titled “The Luna Moth Files” appeared around 5 October 2026 and claimed to expose internal material belonging to Silent Ransom Group (SRG), also tracked as Luna Moth and UNC3753. The published package presents chat exports, a vishing document, screenshots, a purported fake employee résumé, targeting material, and financial claims. The site’s authorship and the full archive’s chain of custody remain unknown; its claims should therefore be treated as an unverified primary-source disclosure rather than fact.

The exposure’s main value is not evidence of a new exploit or ransomware payload. Instead, it offers a view of how a social-engineering-led extortion operation may be organized behind the scenes. The material depicts a workflow built around target research, credible business personas, prepared callers, live coordination with technical operators, victim-authorized remote access, data theft, and structured extortion negotiations. Several of these elements align closely with behavior previously documented by the FBI and other security vendors.

The chats also suggest that Luna Moth’s model extends beyond isolated vishing calls. Discussions reference dedicated telephony infrastructure, commercial business-intelligence services, victim-specific rooms, recruitment efforts, fake-employee concepts, and possible field activity. Taken together, the material portrays an operation seeking to industrialize human-enabled access: distinct participants prepare identities and infrastructure, conduct calls, support remote sessions, manage victims, and coordinate monetization.

The exposure does not validate every claim made by the onion site. Its displayed message counts conflict, and its headline financial total does not reconcile cleanly with the amounts shown in its own table. Claims concerning operator identities, confirmed payments, and deepfake use require independent corroboration. Nevertheless, the archive is internally detailed and behaviorally consistent enough to provide a useful—if provisional—view of the group’s operating model.

CENTRAL ASSESSMENT

The new exposure suggests Luna Moth’s primary innovation is organizational rather than technical: a repeatable, role-based process for turning researched identities and trusted business context into remote access, stolen data, and extortion leverage.

CHAPTER 02

Introduction

Silent Ransom Group is a financially motivated data-extortion operation tracked by security vendors under several names, including Luna Moth and UNC3753. Although commonly discussed within the ransomware ecosystem, the group's documented model generally does not depend on encrypting victim systems. Instead, it uses social engineering to obtain access, steals sensitive information, and pressures organizations to pay by threatening disclosure or sale.

Unit 42 documented the activity in 2022 as a callback-phishing campaign in which personalized subscription invoices directed recipients to attacker-controlled phone numbers. During the resulting calls, victims were persuaded to begin remote-support sessions using legitimate administration software. The operators then searched for valuable information, removed it, and demanded payment.

Later reporting described an evolution toward direct impersonation of a victim organization's internal IT staff. Mandiant documented calls using help desk or data-migration pretexts, screen sharing, legitimate remote-management tools, and consumer file-sharing services. The FBI also reported cases in which individuals posing as IT personnel attempted physical access after remote social engineering failed.

Why the exposure matters. Public reporting established what Luna Moth does. The newly exposed material potentially adds the missing operational layer: how targets are prepared, how callers are coached, how participants coordinate, and how victims move through the extortion process.

CHAPTER 03

The Luna Moth Files

The onion site appeared around 5 October 2026. The captured page presents itself as a press kit and full archive of Silent Ransom Group activity. It claims to contain thousands of messages from two chat servers, dozens of attachments, and Bitcoin wallets, along with material related to victims, operators, vishing, recruitment, and payment activity.

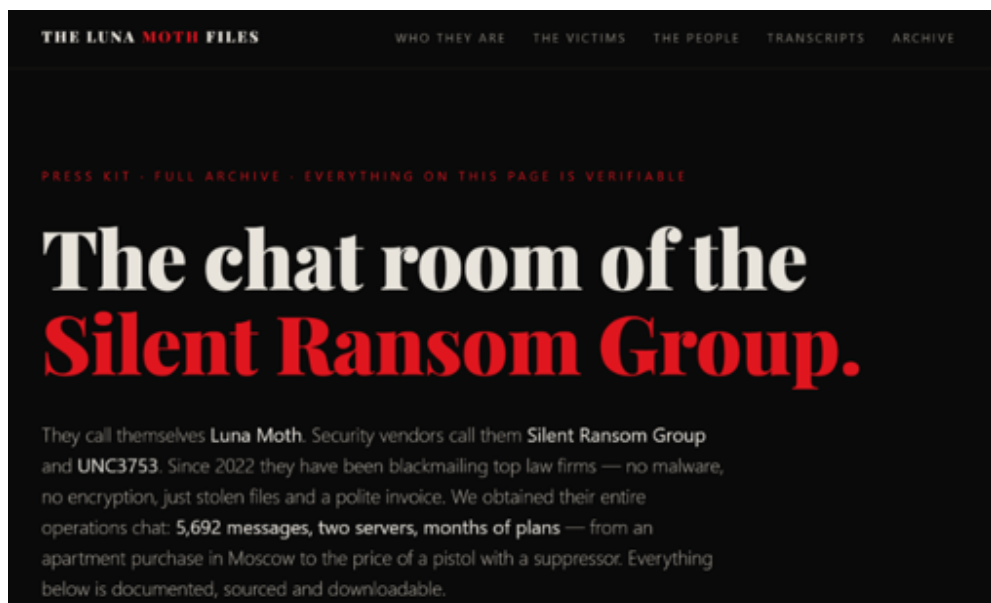


Figure 1: The Luna Moth Files Exposure Onion Site.

The published archive list includes a structured chat export, a Russian-language vishing document, a purported fake IT-employee résumé, targeting material, victim and negotiation screenshots, and photographs described by the author as evidence of field activity. The disclosure is notable because it attempts to connect each stage of the group's operation—from target research to monetization—within one dataset.

What the site claims to provide

Artifact category	Claimed intelligence value
Chat archive	Operational planning, task allocation, infrastructure, target discussions and victim management.
Vishing material	Caller preparation, emotional manipulation and coordination during remote sessions.
Screenshots	Purported victim dossiers, negotiations, workflow stages and field activity.
Fake CV and identity material	Possible recruitment, impersonation or attempted placement of trusted personnel.
Financial claims	Alleged ransom demands, payment states and cryptocurrency handling.

The site's numerical claims require caution. It displays two different message totals, and the financial amounts shown do not clearly reconcile with the headline aggregate. These inconsistencies do not invalidate the entire archive, but they limit confidence in the site author's summary statistics and payment assertions.

CHAPTER 04

What the Exposure Reveals

4.1 Luna Moth appears to operate as a specialized service chain

The leaked material portrays a segmented operation rather than a single caller carrying out every stage. The chats include discussions of target preparation, technical infrastructure, calling activity, victim communication, recruitment, and field-oriented projects. This supports an assessment that different participants contribute distinct capabilities, even though the archive does not establish a formal hierarchy.

The vishing document reinforces this division of labor. It instructs the caller to monitor a separate group chat throughout the remote session and relay changes in the victim's behavior, implying that the person maintaining the conversation may be supported by another operator working on the endpoint.

WHAT THIS ADDS

Previous reporting showed a repeatable vishing pattern. The exposure suggests that repeatability is supported by internal specialization and real-time collaboration, making the operation closer to a coordinated service business than an improvised fraud call.

Roles within the service chain

**Target researchers & persona builders**

Prepare credible business context.

**Callers**

Establish authority and maintain the victim relationship.

**Technical participants**

Support remote sessions and data access.

**Negotiators & payment handlers**

Manage the monetization stage.

4.2 Target research is treated as operational infrastructure

The archive suggests that credibility is built before the first call through business intelligence, fabricated identities and supporting web assets.

Early chat messages discuss creating long-lived domains, business email accounts and simple commercial-looking websites. Other exchanges reference registration for commercial people-data services and contain lists of senior personnel followed by requests to initiate calls.

This pattern suggests the group's access model starts with detailed organizational research. The intended caller is not approaching a random employee; the operation appears to identify high-value organizations, profile relevant personnel, and construct an identity that can survive basic scrutiny.

- Commercial and open-source data supports target selection.
- Business email and web presence strengthen fabricated personas.
- Prepared contact lists make calling campaigns systematic rather than opportunistic.

4.3 The vishing playbook is built around emotional control

The disclosed script describes a deliberate sequence of anxiety, reassurance, and renewed urgency. The caller is instructed to present confidently as internal IT, report suspicious activity, reassure the employee that a malicious message was blocked, and then restore urgency by claiming that other employees compromised the network. Remote access is framed as a protective security check rather than an attacker's request.

The caller is also told to understand the remote-access application thoroughly, keep the victim calm, monitor the operator chat continuously, and finish with a benign explanation for the activity on the device. The script therefore functions as a behavioral playbook, not merely a list of lines to read.

This approach is consistent with publicly documented Luna Moth activity involving internal-IT impersonation, legitimate remote tools, and victim-authorized access. The newly exposed material adds detail about how the caller is coached to manage trust and resistance throughout the interaction.

4.4 Telephony and live coordination are core capabilities

Calling appears to be supported by dedicated infrastructure and an operator backchannel. The chats reference virtual servers intended for 3CX, while the vishing document directs the caller to remain connected to a group chat during the session.

The apparent separation between conversation management and technical activity helps explain how the group can maintain a convincing, calm interaction while another participant searches the victim environment.

WHAT THIS ADDS

The human layer is not separate from the technical intrusion. In the exposed workflow, the call acts as the control channel that keeps the victim cooperative while access and collection occur in parallel.

4.5 Victims appear to move through a structured extortion pipeline

The exposed chats reveal a commercial-style approach to victim management: a structured sequence of negotiation and monetization stages, rather than treating each extortion case as an isolated operation. The archive includes labels such as "CHAT," "OFFER," "CONTRACT," and "GOLD," alongside victim-specific discussions, revenue estimates, negotiation states, and requests for cryptocurrency wallets.

The conversations also provide additional context around how targets are selected, with repeated references to the legal sector and an ambition to target the top 100 law firms globally. This focus is strongly reflected in the group's victimology: 42 of its 50 most recently observed victims were law firms, while Business Services accounts for 69 classifications across the broader dataset, followed by Finance with 22 and Real Estate with two.

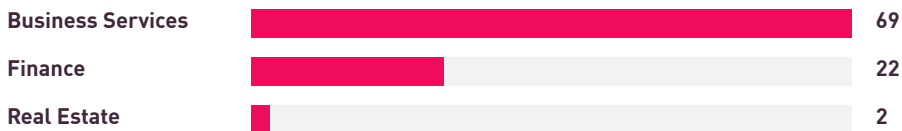


Figure 2: Sector distribution of observed Silent Ransom Group victims. Business Services is heavily represented by law firms.

4.6 The operation may be expanding beyond remote vishing

Fake-employee, recruitment and field-oriented discussions point to experiments with more durable human access.

The archive includes conversations concerning recruitment, prospective agents and a project described as "Fake_Employee." The onion page also lists a purported résumé sent to law firms and photographs it describes as evidence of field activity.

These materials are consistent with the FBI's independent reporting that SRG has attempted physical access by sending individuals posing as IT personnel to victim locations. They may indicate an effort to create alternative access paths when remote social engineering is insufficient.

The evidence is strongest for the existence of internal discussions and project concepts. It is weaker for the successful placement of fake employees or the identity and role of specific individuals shown in the leaked material.

4.7 The exposure provides a view into Luna Moth's internal operations

Most of the core behavior was already visible publicly; the new contribution is the view inside the process. The leaked conversations provide additional context around how targets and personas are prepared, how callers coordinate with other members during active engagements, how victims are tracked through the extortion process, and how recruitment and field-based initiatives may complement the group's established vishing activity.

Rather than revealing a fundamentally new attack chain, the exposure helps connect previously observed techniques into a broader operational picture. If authentic, the material suggests that Luna Moth's effectiveness is supported by a structured division of responsibilities and a collaborative workflow spanning target research, social engineering, technical activity, victim management, and extortion.

ANALYTICAL TAKEAWAY

Luna Moth's advantage appears to come from process discipline: research, credibility, coordinated human interaction, and fast monetization. The exposure makes that operating system visible.

CHAPTER 05

Reconstructed Operating Workflow

The following workflow combines behavior independently documented by the FBI, Mandiant, and Unit 42 with additional organizational detail alleged by the October 2026 exposure. It is presented at a high level and does not reproduce the leaked script or operational instructions.

01**Target research & persona building**

Business intelligence and open-source data select targets and build credible fabricated identities.

**02****Vishing call & victim-authorized access**

A prepared caller impersonates internal IT, manages trust, and persuades the victim to start a remote session.

**03****Technical collection & data theft**

A technical operator searches the environment in parallel while the caller keeps the victim calm.

**04****Victim management & negotiation**

The victim is tracked through staged negotiation states as stolen data is converted into leverage.

**05****Monetization**

Payment is pursued through cryptocurrency handling, without ransomware encryption.

Figure 3: Reconstructed Luna Moth operating workflow.

The sequence illustrates why the group can operate without ransomware encryption. The organization's leverage is created through a chain of trusted context, victim-approved access, selective data theft, and structured pressure.

CHAPTER 06

Conclusions

The October 2026 exposure does not fundamentally change what is known about Luna Moth's technical methods. The operation was already associated with callback phishing, direct IT impersonation, legitimate remote-access tools, rapid data theft, and extortion without encryption. What the new material changes is the level of visibility into how those methods may be organized and repeated.

The disclosed chats and vishing material portray a process-driven operation that invests in target intelligence, fabricated business context, telephony, caller preparation, live support, and victim management. Recruitment and fake-employee discussions suggest that the group may also be exploring ways to extend social engineering into physical or employment-based access. Although these elements require further validation, they fit the group's broader preference for persuading trusted users rather than defeating security controls through malware.

What distinguishes the model is therefore not a technical breakthrough, but the industrialization of human-enabled access. Luna Moth appears to treat social engineering as a coordinated production process: research creates credibility, callers convert credibility into access, technical operators turn access into stolen data, and negotiators convert data into leverage. In that sense, the exposure offers a rare view of how a modern extortion operation can scale around people, process, and legitimate tools rather than ransomware code.

FINAL ASSESSMENT

If authentic, the exposure shows that Luna Moth should be understood less as a conventional ransomware crew and more as a specialized data-extortion business whose core platform is the coordinated manipulation of trust.

About Check Point Exposure Management

Check Point's exposure management changes the game.

We combine billions of internal telemetry points with billions of external signals from the open, deep, and dark web to deliver a unified intelligence fabric. This provides clear visibility across the full attack surface, including brand risk.

The industry is moving from fragmented feeds to real context and real priorities. We support that shift through active threat validation, confirmation of compensating controls, and deduplication across tools, so teams can focus on what actually matters.

With safe-by-design remediation, fixes aren't just assigned, they're implemented. Every fix is validated before enforcement, enabling measurable risk reduction without downtime.

Gartner predicts organizations adopting continuous threat exposure management with mobilization will see 50% fewer successful attacks by 2028. We're leading that shift with action, not just tickets, and Fortune 500 organizations across major industries already rely on Check Point Exposure Management.

Visit checkpoint.com/exposure-management →

ISRAEL

Tel: +972-73-226-4555
5 Shlomo Kaplan Street
6789159

USA

Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE

Tel: +65-6435-1318
78 Shenton Way, #09-01
Tower 1, Singapore 079120

PHILIPPINES

Tel: +63-2-8465-9200
Unit 2005, 20th Floor, Zuellig
Building,
Makati Avenue cor. Paseo de
Roxas,
Makati City 1223, Metro Manila

UK AND IRELAND

Tel: +44-20-7628-4211
85 London Wall, 4th Floor
London, EC2M 7AD

JAPAN

Tel: +81-3-6205-8340
Toranomon Kotohira Tower
25F,
1-2-8, Toranomon, Minato-ku,
Tokyo 105-0001