ZEROFOX INTELLIGENCE

Profile

ICARUS

P-2026-06-26a

Classification: TLP:GREEN

Criticality: Medium

Intelligence Requirements: Threat Actor, Ransomware, Dark Web

June 26, 2026

Profile | ICARUS

Created on: June 26, 2026
Intelligence Cut-off: 7:00 AM (EDT) on June 26, 2026

Key Findings

- ZeroFox first observed ransomware and digital extortion (R&DE) collective ICARUS's data leak site (DLS) and associated extortion campaigns in late April to early May 2026. Since becoming active, the group has listed at least three confirmed targets and five additional redacted entities on its DLS, suggesting ongoing and expanding operations as of mid-2026.
- The operators of "The Underground _ Uwu" Telegram channel have reposted ICARUS's original leak post and have previously claimed affiliations with Scattered Lapsus$ Hunters (SLH); this raises the possibility of an affiliation between ICARUS and SLH. However, ICARUS has not publicly acknowledged or claimed any such affiliation.
- ICARUS is very likely financially motivated. Neither its DLS communications nor its observed operational behavior indicate any political stance, ideological messaging, or affiliation with a specific cause.
- ZeroFox has observed that ICARUS employs a multitiered extortion model centered on supply chain compromise, data exfiltration, and public disclosure threats.
- ZeroFox assesses that ICARUS is likely an operationally immature threat actor group based on multiple observed operational security (OPSEC) lapses. Despite presenting a polished public-facing DLS, the group's operational conduct reflects significant inconsistencies that suggest limited experience relative to more established R&DE collectives.

First Observed	Late April / Early May 2026
Origin	Unknown
Alias	“mr bean” (email)
Motivation	Financial Gain
Targeted Industries	- Finance - Professional services - Technology
Targeted Nations	- United States - Canada - Indonesia - Switzerland
Tools	- Rbfs ransomware (unconfirmed) - OAuth token harvesting - Automated REST Application Programming Interface (API) exfiltration - Gofile (public file hosting) - Session encrypted messaging
	Note: This list should not be treated as exhaustive.

ICARUS overview

Source: ZeroFox Intelligence

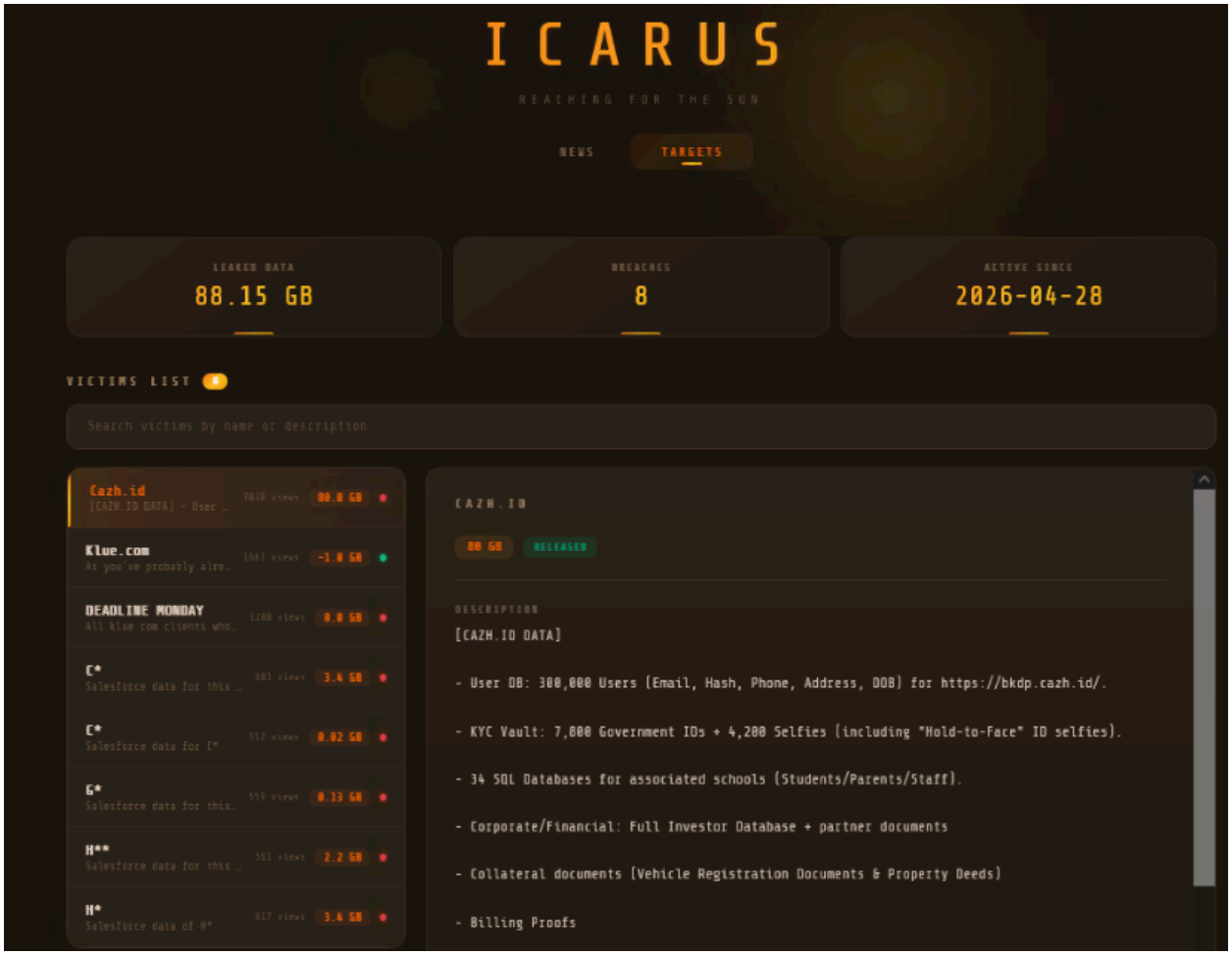
History

ZeroFox first observed R&DE threat actor ICARUS’s initial DLS footprint and associated extortion campaigns in late April to early May 2026. Since becoming active, the group has listed at least three confirmed targets and five additional redacted entities on its DLS, suggesting ongoing and expanding operations as of mid-2026.

- ICARUS's DLS is a polished, mythologically themed platform hosted on the Tor network. ZeroFox has observed the group using the site to publish stolen data and

communicate publicly with victims and observers. Despite its professional appearance, the site exhibits notable backend inconsistencies, including textual placeholders—such as phrases like "DATA ENCRYPTED" or "SF data"—inserted into listings prior to actual file samples being provided, as well as countdown timers displaying anomalous durations of up to 70,000 days within victim posts.

- The group relies on free, public file-sharing services—notably Gofile—to host allegedly exfiltrated data referenced in its DLS posts. This reliance on unstable third-party infrastructure is likely indicative of low operational maturity.
- ICARUS communicates with victims via direct email channels in addition to the DLS. We have observed a consistent email alias of "mr bean" used in private communications with downstream targets of the group's claimed Klue supply chain compromise.
- On June 22, 2026, a Telegram channel operating under the name The Underground _ Uwu published content promoting the Klue data breach previously claimed by ICARUS, appearing to replicate the original leak post verbatim. The post contained two Session contact identifiers—one associated with The Underground _ Uwu, the other linked to ICARUS—suggesting a potential coordination relationship between the two entities.



Homepage of ICARUS's leak site

Source: ZeroFox Intelligence

Potential Affiliations and Associations

The operators of The Underground _ Uwu Telegram channel have previously claimed affiliations with SLH and posted ICARUS's original leak post verbatim, raising the possibility of affiliations between ICARUS and SLH. However, ICARUS has not publicly acknowledged or claimed any such affiliation.

- ZeroFox has historically observed SLH and its affiliates claiming responsibility for cyber incidents originally attributed to other threat actors. As a result, any direct association between ICARUS and SLH remains inconclusive at this stage and should be treated as circumstantial pending further corroborating evidence.

- The overlap in Session identifiers observed in the June 22, 2026, Telegram post represents the strongest current indicator of a potential coordination relationship between The Underground _ Uwu and ICARUS. ZeroFox will continue to monitor for any developments.

Motivations and Victimology

ICARUS is very likely financially motivated. Neither its DLS communications nor its observed operational behavior indicate any political stance, ideological messaging, or affiliation with a specific cause. The group's victim selection pattern indicates opportunistic targeting with a strategic focus on organizations participating in shared digital infrastructure, particularly software-as-a-service (SaaS) integration ecosystems.

- The group's operational focus on supply chain vectors suggests a deliberate strategy of maximizing downstream impact from a single point of compromise. By targeting shared SaaS integration platforms, ICARUS is likely able to affect a broad range of enterprise clients without needing to compromise each organization individually.
- ICARUS appears to favor organizations with significant third-party integration dependencies, particularly those relying on shared OAuth-based authentication frameworks and legacy API credentials—environments that likely present wider attack surfaces and more complex incident response challenges.

Organization	Description	Sector
Cazh	Indonesia-based fintech infrastructure provider	Technology
The Credit Pros	U.S.-based credit repair and financial services firm	Financial Services
Klue	Canada-based business-to-business (B2B) SaaS competitive intelligence platform	Technology
Huntress	U.S.-based managed detection and response provider	Cybersecurity
Gms-net (GMS)	Switzerland-based artificial intelligence (AI)-driven communication solutions	Technology
HDS (Hdscorp)	U.S.-based B2B consulting firm	Professional services
Tata Electronics	Major electronics manufacturer (via third-party vectors)	Manufacturing
Cbassociations	Unidentified entity	Unknown
Cqcrm	Unidentified entity	Unknown

List of alleged organizations targeted by ICARUS

Source: ZeroFox Intelligence

The Klue supply chain compromise is the most significant confirmed incident associated with ICARUS to date. ZeroFox has observed that the following downstream organizations were reportedly impacted as a result of the Klue breach:

- Recorded Future – U.S.-based threat intelligence and cyber-analytics platform
- LastPass – U.S.-based password management and identity security provider
- Tanium – U.S.-based endpoint management and cyber hygiene company
- Jamf – U.S.-based enterprise software provider specializing in Apple mobile device management
- HackerOne – U.S.-based vulnerability coordination and bug bounty platform
- Snyk – U.S.-based developer security company focused on software supply chain safety
- OneTrust – U.S.-based enterprise software firm handling privacy compliance and risk management
- Sprout Social – U.S.-based social media analytics and management platform

- Insurity – U.S.-based cloud software and analytics provider for the commercial insurance industry
- Gong – U.S.-based revenue intelligence and conversational AI sales platform
- Huntress – U.S.-based cybersecurity company specializing in managed detection and response

Tactics, Techniques, and Procedures (TTPs)

ICARUS almost certainly employs a multitiered extortion model centered on supply chain compromise, data exfiltration, and public disclosure threats. ZeroFox has observed that the group's attack chain begins with the exploitation of legacy third-party integration credentials to gain initial access, followed by automated data exfiltration targeting SaaS and customer relationship management (CRM) environments. ICARUS then contacts victims directly using the "mr bean" email alias during extortion negotiations. Consistent with its multitiered extortion approach, the group leverages the threat of publishing stolen data on its DLS to pressure organizations into compliance, even if victims independently restore access to affected systems.

- ICARUS's DLS exhibits textual placeholders within victim listings—including phrases such as "DATA ENCRYPTED" or "SF data"—inserted prior to actual file samples being provided. This behavior indicates an incomplete or ad hoc publication process inconsistent with the site's otherwise polished aesthetic.
- The group has configured ransom countdown timers within victim posts showing durations of up to 70,000 days, a clear operational anomaly that further undermines the credibility and professionalism of the group's public communications.
- ICARUS relies on free public file-sharing services such as Gofile to host allegedly stolen data referenced in DLS postings, suggesting either low operational resourcing or an inability to maintain stable, dedicated infrastructure for data exfiltration hosting.
- The consistent use of the informal email alias "mr bean" for victim communications represents an additional indicator of limited operational

maturity and a failure to adopt professional or obfuscated contact mechanisms typical of more established extortion actors.

ZeroFox has observed the following MITRE ATT&CK techniques used in association with ICARUS activity:

Technique ID	Description
T1195	Supply Chain Compromise – Third-party vendor ecosystem exploitation
T1078.004	Valid Accounts: OAuth Tokens – Harvesting and pivoting on long-lived OAuth tokens disguised as legitimate integrations
T1020	Automated Exfiltration – Executing automated REST API queries to extract files and system metadata at scale
T1071.001	Web Service: Network API – Targeting Salesforce CRM and other SaaS API environments for data access
T1657	Multitiered Extortion – Threatening public data disclosure to pressure victims into ransom payment
T1486	Data Encrypted for Impact – Referenced on DLS; confirmed ransomware deployment has not been verified but cannot be ruled out

ICARUS observed and assessed MITRE ATT&CK techniques
Source: ZeroFox Intelligence

Deep and Dark Web Presence

ICARUS maintains a dedicated Tor-hosted DLS as its primary public-facing infrastructure. The site employs a mythologically themed design and is used both to publicize stolen data and to serve as a platform for communicating with the public and victims. The group also communicates directly with victims via email.

- The DLS lists victim organizations with countdown timers indicating deadlines for ransom payment, after which ICARUS threatens to publish stolen data. The anomalous timer configurations ZeroFox has observed (including values up to 70,000 days) indicate backend configuration issues or deliberate manipulation of deadline communications.

- ICARUS's public messaging on the DLS adopts a mocking tone toward victims, while simultaneously exhibiting significant inconsistencies in the quality and completeness of published content, supporting ZeroFox's assessment of the group as operationally immature.
- ZeroFox has not observed the group recruiting affiliates or soliciting operational support through dark web forums at the time of this report, distinguishing it from groups such as NightSpire that have engaged in public forum-based recruitment.

Indicators of Compromise (IOCs)

The following indicators are derived from telemetry surrounding the confirmed compromise of Klue and its downstream environments, as well as the actor's DLS. Organizations are encouraged to review these indicators and compare them against their own environments and telemetry sources.

Type	Indicator / Value
IP Address	138.226.246[.]94 — Observed infrastructure IP associated with supply chain campaign activity
IP Address	212.86.125[.]24 — Observed infrastructure IP associated with supply chain campaign activity
IP Address	213.111.148[.]90 — Observed infrastructure IP associated with supply chain campaign activity
IP Address	94.154.32[.]160 — Observed infrastructure IP associated with supply chain campaign activity
User-Agent	Python-urllib/3.12 — Suspicious user-agent observed in API logs querying CRM REST paths
User-Agent	Python-urllib/3.14 — Suspicious user-agent observed in API logs querying CRM REST paths
User-Agent	5238 — Suspicious user-agent string observed in API logs querying CRM REST paths
Session ID	0530cecee355f7d0723f3990c6bfb562e29829687f16b5840ad85e18ebc80c6d6b
Session ID	05117e1c4110e0edc5ca1c539784c6a03eb34206e8ef25a8b7a729b4bb0e1a4251
TOX ID	DA823E474381B628529523006FDE05911FE63D80F76E5025968DA9E45F6F0937BB5C92E0CF16

Type	Indicator / Value
IP Address	138.226.246[.]94 — Observed infrastructure IP associated with supply chain campaign activity
Onion / DLS	hXXp://e6ujsppajgb756x7x5ykdryvlcjynltb52eiwi6pd4bfwo6hddd6neid[.]onion/
Email Alias	"mr bean" — Consistent email alias used in private victim communications

ICARUS IOCs
Source: ZeroFox Intelligence

Assessment

ZeroFox assesses that ICARUS is an operationally immature threat actor group based on multiple observed OPSEC lapses. Despite presenting a polished public-facing DLS, the group's operational conduct reflects significant inconsistencies that suggest limited experience relative to more established R&DE collectives.

Despite the sophistication of the initial attack vector—specifically, the exploitation of long-lived OAuth tokens to execute a multistage supply chain compromise against Klue and its downstream clients—the group's post-compromise conduct and public communications demonstrate a level of operational inexperience inconsistent with the technical capability implied by that initial access. ZeroFox assesses that ICARUS likely benefits from a narrow area of technical proficiency, possibly acquired or outsourced, that does not reflect the group's overall maturity.

The potential affiliation with Scattered Lapsus$ Hunters, if confirmed, would indicate access to a broader network of operational support, tooling, or targeting intelligence. However, given SLH's history of opportunistically claiming association with incidents attributed to other actors, ZeroFox views this relationship as inconclusive and will continue to assess it as new information becomes available.

ICARUS remains an active threat as of mid-2026. Organizations participating in shared SaaS integration ecosystems—particularly those relying on OAuth-based third-party access—should treat this group as a credible and ongoing risk. The group's

demonstrated ability to achieve significant downstream impact from a single supply chain compromise warrants continued monitoring, regardless of its assessed operational immaturity.

Recommendations

- Audit and revoke all legacy API keys, OAuth tokens, and shared integration credentials connected to third-party SaaS vendors. Implement token rotation policies and enforce time-limited credential scopes where possible.
- Implement robust logging and data-exfiltration monitoring across all shared digital infrastructure, particularly for REST API activity, to quickly detect and isolate unauthorized access consistent with ICARUS's observed tooling.
- Review and restrict third-party integrations, ensuring that vendor access follows the principle of least privilege and that long-lived integration tokens cannot be used to pivot into downstream environments.
- Develop a comprehensive incident response strategy that specifically addresses supply chain compromise scenarios, including downstream client notification procedures.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web forums, including references to organizational assets on known extortion-focused DLS platforms.
- Implement network segmentation to limit lateral movement opportunities from compromised integration points into core organizational infrastructure.
- Ensure critical, proprietary, or sensitive data is backed up to secure, off-site or cloud servers regularly, and verify that backup integrity cannot be compromised via the same OAuth or API access pathways used in normal operations.
- Leverage cyber threat intelligence to inform detection engineering for ICARUS-associated TTPs, particularly automated API query behavior originating from Python-based user-agents targeting CRM environments.

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%