ZEROFOX INTELLIGENCE

# Flash

## Grafana Labs Source Code Theft and Extortion Attempt

F-2026-05-20a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Threat Actor, Ransomware, Digital Extortion

May 20, 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 10:00 AM (EDT) on May 20, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

# | Flash | Grafana Labs Source Code Theft and Extortion Attempt

## | Key Findings

- On May 17, 2026, Grafana Labs disclosed that its private code was stolen from a GitHub repository using a known vulnerability called a "Pwn Request." The breach was claimed by ransomware and digital extortion (R&DE) collective CoinbaseCartel; however, Grafana Labs refused to pay the ransom demanded.
- CoinbaseCartel first appeared in September 2025, focusing exclusively on data theft and extortion—removing proprietary information from servers before demanding ransom.
- CoinbaseCartel reportedly shares infrastructure, including a domain, with the Scattered Lapsus$ Hunters (SLSH) ecosystem, suggesting it is very likely an offshoot of the SLSH and likely operates as the data theft extortion affiliate for the larger SLSH collective.
- This attack very likely signifies a further diversification within the SLSH ecosystem. SLSH is already the dominant English-language R&DE collective and has previously splintered into specializations; more brand diversification within the ecosystem is very likely in 2026 and beyond.

## Details

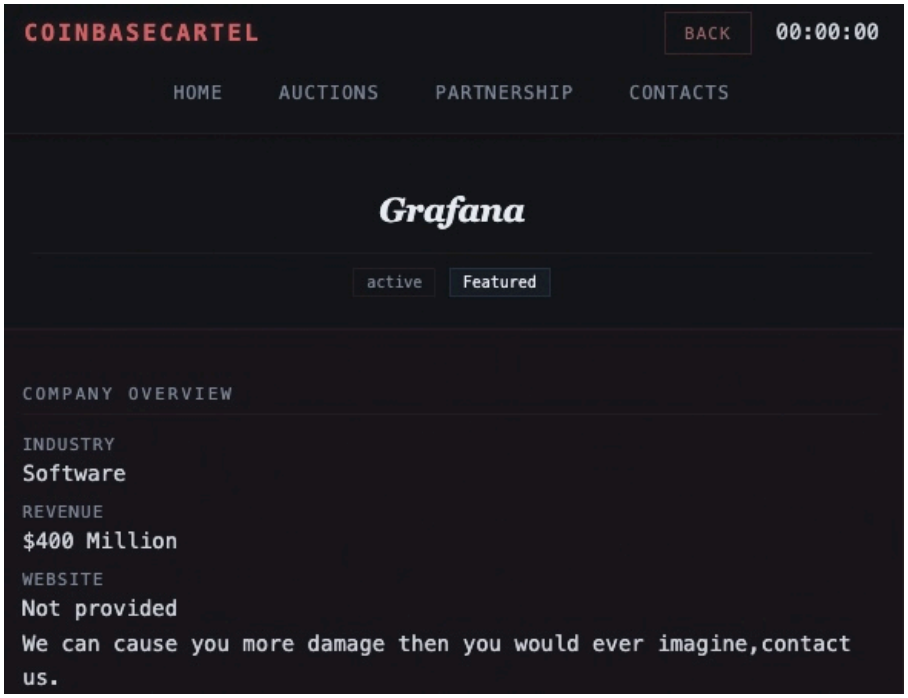
On May 17, 2026, Grafana Labs disclosed a threat actor exploited a misconfigured GitHub Actions workflow known as a Pwn Request to steal a privileged GitHub App token. This exploit allowed the actor to exfiltrate Grafana's private source code and attempt to extort the company.[1]

- A Pwn Request is a software development vulnerability specific to GitHub Continuous Integration and Continuous Delivery (CI/CD) automated workflow pipelines. It occurs when a workflow auto-executes untrusted code submitted by external contributors, giving an attacker full access to repository secrets and write permissions.

Coinbase Cartel—a data theft-only extortion collective that is likely a splinter of the SLSH ecosystem—publicly claimed the attack on Grafana Labs on its dark web leak site. The collective reportedly demanded an undisclosed ransom, which Grafana Labs refused to pay—citing Federal Bureau of Investigation (FBI) guidance on ransomware negotiations, which states that paying ransoms does not guarantee the return of stolen data.[2]

[1] hXXps://thehackernews[.]com/2026/05/grafana-github-token-breach-led-to.html

[2] hXXps://www.techzine[.]eu/news/security/141395/grafana-refuses-to-pay-ransom-after-source-code-stolen-via-github-token/




**CoinbaseCartel's claim of responsibility**

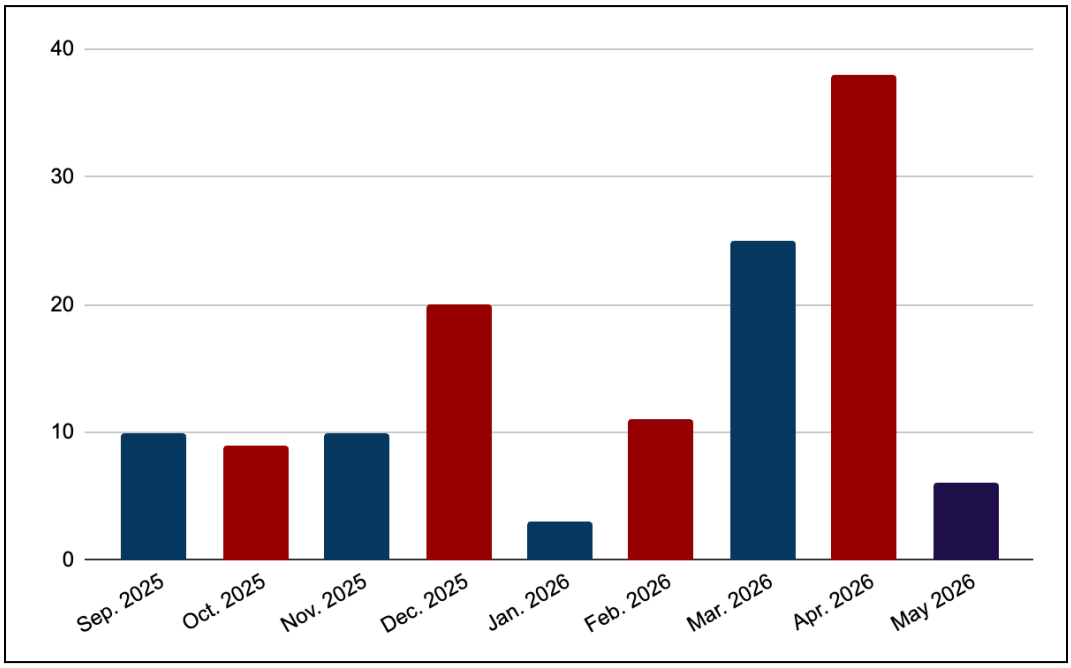
*Source: ZeroFox Intelligence*

CoinbaseCartel reportedly exploited a vulnerability in a recently enabled workflow in the "grafana/grafana" repository.[3] The event was triggered by pull request events native to GitHub, which then ran with elevated permissions to secret repositories. This action is done by exploiting a known vulnerability in the GitHub platform, which allows for elevated permissions on certain automated workflows, as long as the request originates from an external fork.

- Once the Grafana repository was forked, the threat actor was able to craft a malicious script injection payload, encrypt the codebase with a private key, extract Grafana's private code, delete the fork to cover their tracks, and duplicate four additional private repositories.[4]
- According to Grafana Labs, no personal or customer information was compromised in the breach.[5]

[3] hXXps://www.cyberkendra[.]com/2026/05/grafana-labs-refuses-ransom-after.html
[4] *Ibid.*
[5] hXXps://www.securityweek[.]com/grafana-confirms-breach-after-hackers-claim-they-stole-data/

CoinbaseCartel first appeared in September 2025, focusing exclusively on data theft and extortion; the group does not encrypt data and instead removes proprietary information from servers before demanding a ransom.[6] Since its inception, CoinbaseCartel has been responsible for at least 134 incidents—an average of over 16 attacks per month. The collective has attacked organizations across healthcare, technology, transportation, manufacturing, and professional services.




**CoinbaseCartel attacks by month**

*Source: ZeroFox Intelligence*

CoinbaseCartel reportedly shares infrastructure, including a domain, with SLSH, suggesting it is very likely an offshoot of the SLSH ecosystem and likely operates as the data theft extortion affiliate for the larger SLSH collective.[7]

[6] hXXps://www.techzine[.]eu/news/security/141395/grafana-refuses-to-pay-ransom-after-source-code-stolen-via-github-token/

[7] hXXps://www.halcyon[.]ai/jp/threat-group/coinbasecartel

This refusal to pay ransom stands in contrast to Instructure, whose online learning management system, Canvas, was breached by ShinyHunters on April 30, 2026.[8] Following that attack, on May 12, 2026, Instructure reached an agreement and very likely paid an undisclosed ransom to prevent further release of its data—or its customers' login credentials, which were almost certainly obtained in the attack.[9]

- In the case of Instructure, it is unlikely that ShinyHunters destroyed all of the exfiltrated data as the group informed its victim it had—leaving hundreds of Canvas clients, including several Fortune-level companies, vulnerable to phishing attacks.

The Grafana Labs code theft is the latest in a series of data theft-only breaches from CoinbaseCartel and very likely demonstrates the viability of its approach. The successful breach of at least 134 victims in just over eight months shows that CoinbaseCartel is almost certainly capable of inflicting damage on corporate targets without the use of encryption. This methodology very likely presents new challenges in ransomware defense—backing up data is no longer secure if publication, rather than encryption, is the goal of the attackers.

Additionally, this attack very likely signifies a further diversification within the SLSH ecosystem. SLSH is already one of the most active and capable English-language R&DE collectives and has previously splintered into specializations—ShinyHunters previously established "shinysp1d3r" as the primary encryptor for the collective.[10] CoinbaseCartel almost certainly represents a further splintering of SLSH into specialized cells, and more brand diversification within the ecosystem is very likely in 2026 and beyond.

[8] hXXps://www.wral[.]com/news/education/canvas-shinyhunters-ransom-instructure-hack-data-breach-may-2026/
[9] hXXps://abc7[.]com/post/deal-reached-hackers-delete-data-stolen-canvas-educational-platform/19086610/
[10] hXXps://www.broadcom[.]com/support/security-center/protection-bulletin/shinysp1d3r-ransomware

## 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 deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (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% |