



| Flash |

Ransomware Recovery CEO Charged for Secret Payments

F-2026-10-13a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Dark Web, Ransomware, Threat Actor

October 13, 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 October 13, 2026**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

| Flash | Ransomware Recovery CEO Charged for Secret Payments

| Key Findings

- On October 7, 2026, the owner and Chief Executive Officer (CEO) of a ransomware recovery company was arrested and charged with one count of conspiracy to commit wire fraud and two counts of wire fraud.
- The CEO allegedly defrauded ransomware victims by claiming to use proprietary technology to recover encrypted data while reportedly paying the attackers for decryption keys.
- A *ProPublica* investigation from 2019 reported that security researchers had created their own ransomware and approached recovery companies posing as victims; the CEO reportedly contacted the fake ransomware group and offered to pay the ransom.
- This fraud and subterfuge incident is almost certainly an isolated example of unscrupulous actors in the cybersecurity industry. Fraud schemes from cybersecurity companies are very likely rare but represent a unique insider threat; they almost certainly present a secondary threat layer that businesses should keep in mind when developing their defensive operations and mitigation plans.

| Details

On October 7, 2026, the owner and CEO of a ransomware recovery company was arrested and charged with one count of conspiracy to commit wire fraud and two counts of wire fraud. The CEO allegedly defrauded ransomware victims by claiming to use proprietary technology to recover encrypted data while reportedly paying the attackers for decryption keys.¹

According to the U.S. Department of Justice (DOJ), the CEO made misrepresentations to ransomware victims by advising them not to pay ransoms and assuring them that his company could recover their encrypted data without the need for ransom payment. Without the victims' knowledge, the CEO would then allegedly contact the cybercriminals responsible for the ransomware and negotiate a lower price for a decryption key.²

The CEO reportedly charged victims much higher rates than they were likely to pay in ransoms and significantly more than his company paid in ransoms to the cybercriminals. For example, in August 2023, the CEO reportedly made a ransom payment of USD 8,200 and then charged the victim USD 150,000 to decrypt their data.³

- Over the course of the alleged scheme, the CEO reportedly charged clients more than USD 19 million, while paying roughly USD 8 million in ransoms.⁴

A *ProPublica* investigation from 2019 reported that security researchers created their own ransomware and approached several recovery companies posing as victims. In at least one instance, the CEO now under indictment contacted the fake ransomware group and offered to pay the ransom.⁵

This fraud and subterfuge incident is almost certainly an isolated example of unscrupulous actors in the cybersecurity industry. While it remains the standing advice of

¹ [hXXps://www.bleepingcomputer\[.\]com/news/security/ransomware-recovery-ceo-charged-over-secret-ransom-payments/](https://www.bleepingcomputer.com/news/security/ransomware-recovery-ceo-charged-over-secret-ransom-payments/)

² [hXXps://www.justice\[.\]gov/opa/pr/known-cybersecurity-expert-and-owner-florida-ransomware-remediation-company-charged](https://www.justice.gov/opa/pr/known-cybersecurity-expert-and-owner-florida-ransomware-remediation-company-charged)

³ *Ibid.*

⁴ [hXXps://www.justice\[.\]gov/usao-edny/pr/owner-florida-ransomware-remediation-company-charged-defrauding-clients](https://www.justice.gov/usao-edny/pr/owner-florida-ransomware-remediation-company-charged-defrauding-clients)

⁵ [hXXps://www.bleepingcomputer\[.\]com/news/security/ransomware-recovery-ceo-charged-over-secret-ransom-payments/](https://www.bleepingcomputer.com/news/security/ransomware-recovery-ceo-charged-over-secret-ransom-payments/)

both the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) not to pay ransoms in the event of an incident,⁶ ZeroFox recommends that victims maintain vigilance when choosing professional mitigation services. Fraud schemes from cybersecurity companies are very likely rare but represent a unique insider threat; they almost certainly present a secondary threat layer that businesses should keep in mind when developing their defensive operations and mitigation plans.

⁶ [hXXps://www.justice\[.\]gov/opa/pr/known-cybersecurity-expert-and-owner-florida-ransomware-remediation-company-charged](https://www.justice.gov/opa/pr/known-cybersecurity-expert-and-owner-florida-ransomware-remediation-company-charged)

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

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.

Amber

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

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.

Clear

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%