



| Flash |

FBI Suspects Ransomware Negotiator Aided ShinyHunters

F-2026-10-21a

Classification: TLP:CLEAR

Criticality: Moderate

Intelligence Requirements: Threat Actor, Dark Web, Ransomware

October 21, 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 21, 2026**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

| Flash | FBI Suspects Ransomware Negotiator Aided ShinyHunters

| Key Findings

- On October 8, 2026, the Federal Bureau of Investigation (FBI) arrested an executive from a Canadian cybersecurity firm in connection with an ongoing investigation into the ShinyHunters ransomware and digital extortion (R&DE) threat collective.
- Another executive from a second cybersecurity company very likely played an active role in shinywire[.]com, the now-defunct ShinyHunters victim extortion site. The shinywire[.]com site was active from at least May 2026 and was no longer online as of October 16, 2026.
- The most recent arrest came two weeks after ShinyHunters claimed a breach of the FBI jobs portal, which contained a reported 2–3TB of data and very likely included personal information on thousands of FBI employees and their families.
- Ransomware negotiators and incident mitigation service providers very likely represent a secondary threat layer, and these most recent examples are not isolated. ZeroFox recommends that victims maintain vigilance when choosing professional mitigation services.

Details

On October 8, 2026, the FBI arrested an executive from a Canadian cybersecurity firm in connection with an ongoing investigation into the ShinyHunters R&DE threat collective.¹ The executive is a prominent ransomware negotiator, but the FBI believes he has close ties with the threat actor—and that he likely ran a website the collective used to pressure victims into paying ransoms.²

Additionally, another executive—from a second cybersecurity company—very likely played an active role in shinywire[.]com, the now-defunct ShinyHunters victim extortion site. The shinywire[.]com site had been active since at least May 2026 but was no longer online as of October 16, 2026. The FBI suspects this second executive also colluded with ShinyHunters to pressure victims into paying ransoms; however, this executive is not being named, as no formal charges have been filed against them at the time of this writing.

Click + to show notice

We exhort you to **reply** and **engage** with us. We seek an amicable and quiet resolution. **Nobody has to know about this.** It is a perfectly resolvable situation if you come and talk to us. We want to resolve this with you confidentially, quietly, amicably, and professionally.

Kindly, do not let the price be an incentive to walk away or not engage with us. We are flexible and lenient. **We follow through on our promises and word for absolute good or bad.**

[illegible]

One section of shinywire[.]com homepage

Source: ZeroFox Intelligence

¹ [hXXps://krebsonsecurity\[.\]com/2026/10/fbi-arrests-founder-of-ransomware-negotiation-firm/](https://krebsonsecurity.com/2026/10/fbi-arrests-founder-of-ransomware-negotiation-firm/)

² [hXXps://krebsonsecurity\[.\]com/2026/10/feds-suspect-ransom-negotiator-ran-shinyhunters-extortion-site/](https://krebsonsecurity.com/2026/10/feds-suspect-ransom-negotiator-ran-shinyhunters-extortion-site/)

The most recent arrest came two weeks after ShinyHunters claimed a breach of the FBI jobs portal, which contained a reported 2–3TB of data and very likely included personal information on thousands of FBI employees and their families.³

- ShinyHunters is a financially motivated R&DE collective of unknown origin that has been active since at least 2020.
- The group operates on a “pay or leak” model; they do not lock victims out of their data or encrypt servers. Instead, a ShinyHunters attack simply copies user, employee, and customer data from the victim and issues a ransom demand; failure to negotiate results in a leak of sensitive data.⁴

The FBI jobs portal breach elicited an unusually rapid reaction from the FBI, with one suspect—a teenager known only as “Rey”—arrested in Jordan on October 3, 2026. Rey very likely assumed control of ShinyHunters following the arrest of the original leaders in France in 2025.⁵ Following his arrest, Rey has reportedly been cooperating with the FBI,⁶ which likely led to subsequent arrests.

Ransomware negotiators and incident mitigation service providers very likely represent a secondary threat layer—and these most recent examples are not isolated. 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 actually paying the attackers for decryption keys.⁷

Many insurance providers suggest victims work with specific incident response firms;⁸ however, most breach response companies are unlikely to facilitate payments to threat actors, based on standing advice from both the FBI and the Cybersecurity and

³ [hXXps://www.bleepingcomputer\[.\]com/news/security/shinyhunters-claims-fbi-hack-data-theft-in-peoplesoft-zero-day-breach/](https://www.bleepingcomputer.com/news/security/shinyhunters-claims-fbi-hack-data-theft-in-peoplesoft-zero-day-breach/)

⁴ [hXXps://www.mayhemcode\[.\]com/2026/03/shinyhunters-hacking-group-explained.html](https://www.mayhemcode[.]com/2026/03/shinyhunters-hacking-group-explained.html)

⁵ [hXXps://www.infosecurity-magazine\[.\]com/news/french-authorities-arrest-four/](https://www.infosecurity-magazine[.]com/news/french-authorities-arrest-four/)

⁶ [hXXps://krebsonsecurity\[.\]com/2026/10/feds-suspect-ransom-negotiator-ran-shinyhunters-extortion-site/](https://krebsonsecurity[.]com/2026/10/feds-suspect-ransom-negotiator-ran-shinyhunters-extortion-site/)

⁷ [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/)

⁸ [hXXps://krebsonsecurity\[.\]com/2026/10/feds-suspect-ransom-negotiator-ran-shinyhunters-extortion-site/](https://krebsonsecurity[.]com/2026/10/feds-suspect-ransom-negotiator-ran-shinyhunters-extortion-site/)

Infrastructure Security Agency (CISA) not to pay ransoms in the event of an incident.⁹ As a result, when victims reach a decision to pay a ransom, they are more likely to be at the mercy of companies willing to deal directly with cybercriminals.

ZeroFox recommends that victims maintain vigilance when choosing professional mitigation services. Unscrupulous actors in the legitimate cybersecurity industry are very likely rare but almost certainly present a unique threat that businesses should keep in mind when developing their defensive operations and mitigation plans.

For its part, the FBI is almost certainly still in the early stages of a very likely prolonged campaign to disrupt ShinyHunters following the September FBI jobs portal breach. FBI Director Kash Patel has previously stated the Bureau will continue to work with international partners to locate and arrest ShinyHunters members “no matter where they operate.”¹⁰ Arrests of ShinyHunters members—as well as takedowns of their infrastructure—are almost certain to continue in the coming months.

⁹ [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)

¹⁰ [hXXps://www.reuters\[.\]com/world/us/fbi-director-patel-says-bureau-has-arrested-another-person-tied-shinyhunters-2026-10-09/](https://www.reuters.com/world/us/fbi-director-patel-says-bureau-has-arrested-another-person-tied-shinyhunters-2026-10-09/)

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%