



| Flash |

ShinyHunters Claims Breach of Sensitive FBI Data

F-2026-09-23a

Classification: TLP:CLEAR

Criticality: Moderate

Intelligence Requirements: Threat Actor, Geopolitical, Dark Web

September 23, 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 3:00 PM (EDT) on September 23, 2026**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

| Flash | ShinyHunters Claims Breach of Sensitive FBI Data

| Key Findings

- On September 22, 2026, prominent ransomware and digital extortion (R&DE) collective ShinyHunters claimed a breach of the Federal Bureau of Investigation (FBI) and defaced the FBI job application web site.
- ShinyHunters claims it exploited an Oracle PeopleSoft zero-day to steal 2–3 TB of data on almost all FBI agents and job applicants; Reuters independently matched details in a sample of the data against public and previously breached records, though the FBI has confirmed only that it is investigating unauthorized activity on fbijobs[.]gov.
- The claim lands amid a rare convergence of geopolitical flashpoints: the run-up to the November 3 U.S. midterm elections, an escalating U.S.–Iran conflict with fighting also intensifying between Saudi Arabia and Iran-backed Houthi forces, and a Russian gray-zone campaign of drone incursions and sabotage against NATO members.
- ShinyHunters is a decentralized, financially motivated brand with no confirmed nation-state affiliation, and the group states its motive is retaliation over a May 2026 FBI advisory. Given the timing, the target, and the precedent set by Rhysida's pre-election breach of Berlin's city government in August 2026, ZeroFox assesses

there is a roughly even chance this incident reflects something beyond retaliation alone: deliberate exploitation of the ShinyHunters brand, wittingly or not, for political interference or intelligence-collection purposes.

- ZeroFox warns the more immediate risk is that ShinyHunters sells the stolen personnel data to criminal or nation-state buyers, who could exploit it for blackmail, targeting of agents' families, or counterintelligence purposes.

| Details

On September 22, 2026, prominent R&DE collective ShinyHunters claimed a breach of the FBI and defaced the FBI job application web site, [fbijobs\[.\]gov](https://fbijobs.gov).¹ The threat actor reportedly conducted the attack by exploiting a new Oracle PeopleSoft zero-day vulnerability, gaining access to data on employees and applicants.²

- PeopleSoft is an enterprise resource-planning software suite created by Oracle that helps large organizations manage complex business operations, including human resources, financials, and supply chains.³

According to reliable media reporting, ShinyHunters says it first breached the PeopleSoft server used for HR and recruiting, then pivoted into an Amazon-hosted government cloud environment storing agent and applicant records.⁴ Reuters examined a sample of roughly 5,000 records the group provided and found that in at least 10 cases—including a record purporting to belong to FBI Director Kash Patel—names and address details matched credit bureau and previously breached data.⁵

- The FBI has confirmed only that it is investigating unauthorized activity affecting [fbijobs\[.\]gov](https://fbijobs.gov); it has not confirmed that internal systems were compromised or verified the scope of the theft—an important caveat given how recently this incident has occurred.⁶

¹ [hXXps://hackread\[.\]com/shinyhunters-hacks-fbi-jobs-portal-fbi-agents-data/](https://hackread.com/shinyhunters-hacks-fbi-jobs-portal-fbi-agents-data/)

² [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/)

³ [hXXps://www.oracle\[.\]com/uk/applications/peoplesoft/](https://www.oracle.com/uk/applications/peoplesoft/)

⁴ [hXXps://techcrunch\[.\]com/2026/09/22/hacking-group-shinyhunters-claims-it-breached-the-fbi-stole-agents-and-applicants-data/](https://techcrunch.com/2026/09/22/hacking-group-shinyhunters-claims-it-breached-the-fbi-stole-agents-and-applicants-data/)

⁵ [hXXps://www.cbc\[.\]ca/news/world/shinyhunters-breach-fbi-9.7354002](https://www.cbc.ca/news/world/shinyhunters-breach-fbi-9.7354002)

⁶ [hXXps://cyberscoop\[.\]com/shinyhunters-claims-fbi-attack/](https://cyberscoop.com/shinyhunters-claims-fbi-attack/)

- ShinyHunters claims the vulnerability allows remote code execution and that, by using it, the threat actor was able to steal 2–3 TB of data.⁷ The data allegedly includes full personally identifiable information (PII), background information, educational records (including grades and degrees), details of previous U.S. government employment, and sensitive medical and drug-related information.⁸



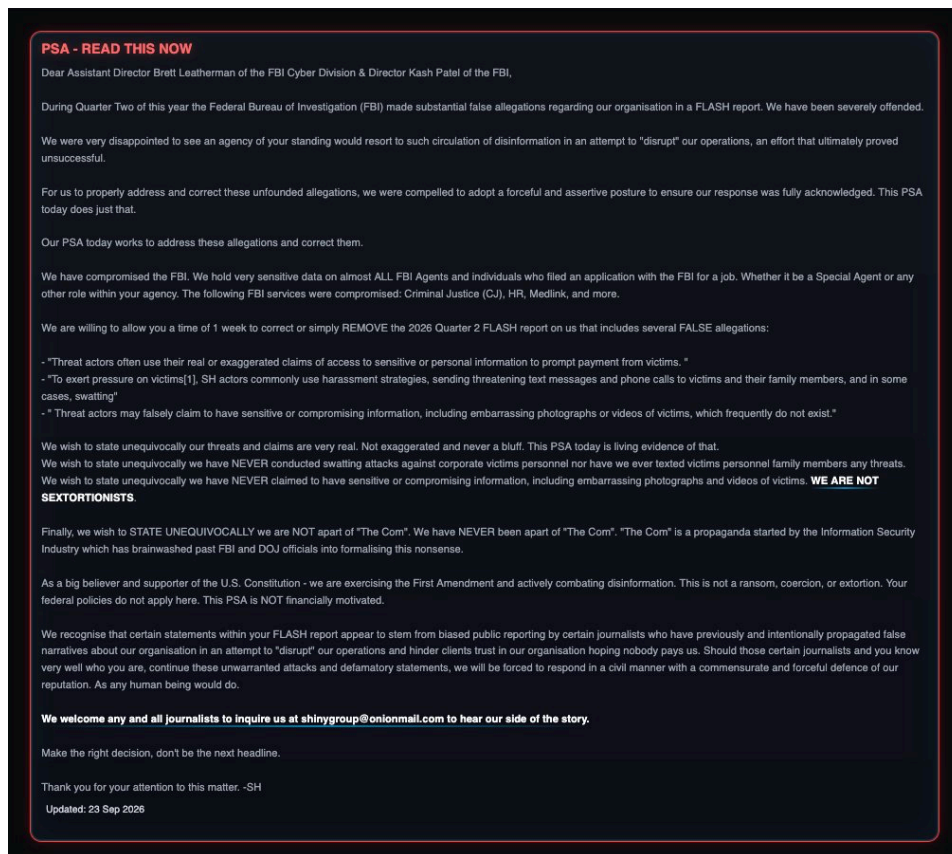
FBI job application portal defaced by ShinyHunters

Source: ZeroFox Intelligence

According to the threat actor, the motivation for the attack stems from a May 2026 FBI report, which ShinyHunters claims contains false information about them. In a message posted to the group's leak site, ShinyHunters states that the breach of the FBI is not extortion, while simultaneously giving the agency one week to correct or remove the threat report.

⁷ [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/)

⁸ [hXXps://hackread\[.\]com/shinyhunters-hacks-fbi-jobs-portal-fbi-agents-data/](https://hackread.com/shinyhunters-hacks-fbi-jobs-portal-fbi-agents-data/)



ShinyHunters' message to the FBI

Source: ZeroFox Intelligence

A Rare Convergence of Flashpoints

The timing of ShinyHunters' disclosure of the alleged breach of the FBI's job application portal comes amid at least three U.S. political flashpoints—a convergence that raises, without resolving, the question of whether ShinyHunters is drifting from a purely criminal collective toward a tool of state interest. The United States will hold midterm elections on November 3, 2026, wherein the entire House of Representatives and roughly one-third of the Senate will be chosen for the next session of Congress.⁹ The FBI breach also lands against a Middle East and Russia-NATO escalatory backdrop that has grown steadily more volatile.

- The United States and Iran remain locked in a military standoff over control of the Strait of Hormuz, and Saudi Arabia and Iran-backed Houthi forces have escalated

⁹ [hXXps://www.usvotefoundation\[.\]org/when-are-2026-midterm-elections-and-what-their-purpose](https://www.usvotefoundation.org/when-are-2026-midterm-elections-and-what-their-purpose)

fighting in Yemen in recent weeks, which has included a Houthi ballistic missile attack toward Riyadh and Houthi seizure of territory along the Bab al-Mandab Strait.¹⁰ The U.S. State Department has warned the conflict could escalate rapidly.

- Simultaneously, Russia has escalated a “gray-zone” campaign against NATO members over the past several weeks that has included drone incursions into Lithuanian and Polish airspace, a Russian drone that washed up on a Polish shore, a near-miss with a Danish helicopter, and suspected sabotage of Dutch rail infrastructure.¹¹
- NATO’s top general said on September 19 that the alliance is prepared for further Russian escalation, describing the activity as an attempt to “undermine trust and weaken our unity.”¹²

Although none of these three flashpoints—the U.S. midterms, the Middle East conflict, or the Russia-NATO gray-zone campaign—is by itself evidence that the ShinyHunters breach of the FBI was directed or timed by a state actor, nation-states have historically used R&DE brands as one of many intelligence tools deployed to conduct low-cost, deniable, and difficult-to-attribute intelligence operations. For example, R&DE collective Rhysida stole data from Berlin State in Germany in the weeks ahead of its elections, likely in an attempt to influence the election.

- ZeroFox notes that influence operations such as data dumping do not necessarily need to affect the election outcome to be considered successful. Generating friction online within the public discourse and news media cycles almost certainly damages Western institutions reputationally during a period of heightened tension, which makes these groups a convenient vector for any actor—state or criminal—seeking to sow distrust in longstanding institutions.

Criminal Brand or Political Vector?

The alleged leaders of ShinyHunters were arrested by French authorities in June 2025. Those arrests were the result of an international investigation into the dark web forum BreachForums and reportedly included significant investigative contributions from the

¹⁰ <https://us.cnn.com/2026/09/20/middleeast/mideast-tensions-un-general-assembly-heres-what-to-know>

¹¹ <https://www.cnn.com/2026/09/17/europe/russia-attacks-europe-misstep-analysis-intl>

¹² <https://www.pravda.com.ua/eng/news/2026/09/19/8054253/index.amp>

FBI.¹³ Whoever is currently operating as ShinyHunters—and thus conducted the September 22 attack on the FBI—is very likely using the name as a brand. There is a roughly even chance that the current operators have nothing to do with the ShinyHunters collective that was disrupted in 2025.

- As of this writing, ShinyHunters itself has no confirmed nation-state base of operations, as it is considered a decentralized, English-language cybercrime ecosystem tied to “the Com,” with arrested affiliates identified in France and elsewhere in Europe and no confirmed central leadership.¹⁴
- Although this profile favors the group’s own stated motive (retaliation over the May 2026 advisory), it also works as plausible cover for intelligence purposes.

ZeroFox warns the more immediate risk is that ShinyHunters sells the stolen personnel data to criminal or nation-state buyers, who could exploit it for blackmail, targeting of agents’ families, or counterintelligence purposes. Data on law enforcement personnel has a well-established espionage value independent of who steals it first: the 2015 breach of the U.S. Office of Personnel Management, attributed to Chinese state-linked actors, remains the clearest precedent for how a government personnel database can be repurposed for counterintelligence rather than extortion.

Weighing the two hypotheses: it is likely that ShinyHunters’ stated grievance against the FBI is genuine and is, at minimum, a contributing driver of this attack. There is a roughly even chance that the group’s brand, timing, or eventual disposition of the stolen data is separately being shaped—wittingly or through opportunistic third-party exploitation—by an actor seeking political disruption or intelligence value rather than pure retaliation. ZeroFox holds no confident view on which state, if any, might benefit, and cautions against reading Russia’s well-documented gray-zone campaign against NATO as evidence of a direct link absent further reporting. This Flash represents ZeroFox’s initial assessment of a fast-moving, largely unconfirmed incident; we will update this analysis as the FBI’s investigation and independent verification of the stolen data progresses.

¹³ <https://www.infosecurity-magazine.com/news/french-authorities-arrest-four/>

¹⁴ <https://www.huntress.com/threat-library/threat-actors/shinyhunters>

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%