



| Flash |

ShinyHunters Continues Shift to Encryption-Less Data Theft

F-2026-09-16a

Classification: TLP:CLEAR

Criticality: Moderate

Intelligence Requirements: Threat Actor, Data Breach, Dark Web

September 16, 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 PM (EDT) on September 15, 2026**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

| Flash | ShinyHunters Continues Shift to Encryption-Less Data Theft

| Key Findings

- On September 10, 2026, threat actor group ShinyHunters leaked data from McKesson Corporation (McKesson) on its dark web leak site. The data allegedly came from an August 2026 breach of 6.4 million personally identifiable information (PII) records associated with McKesson.
- Neither the public disclosures nor the ShinyHunters claim mentioned ransomware or encryption, making it very likely the group did not encrypt McKesson data; instead, ShinyHunters very likely extracted the data, issued a ransom demand, and then almost certainly leaked the data when the victim refused to pay.
- ZeroFox assesses that the lack of encryption in the McKesson breach was almost certainly intentional and very likely represents a tactical shift by ShinyHunters from double extortion to encryption-less data theft.
- The ShinyHunters data breach of McKesson and the subsequent release of sensitive data almost certainly reflect the continuation of the shift in the ransomware and digital extortion (R&DE) ecosystem from encryption-based attacks to “encryption optional” data extortion.

| Details

On September 10, 2026, threat actor group ShinyHunters leaked data from McKesson on its dark web leak site. The data allegedly came from an August 2026 breach of 6.4 million PII records, including email addresses, dates of birth, employers, genders, names, personal health data, phone numbers, and physical addresses belonging to individuals identified as patients, marketing campaign participants, staff, and healthcare providers associated with McKesson.¹

- McKesson is a Texas-based healthcare logistics, pharmaceutical distribution, and health information technology company.²
- McKesson discovered the breach on August 25, 2026, and reported the incident to the Securities and Exchange Commission three days later.³
- ShinyHunters claimed responsibility for the breach and stated it had stolen 1 TB of data over a four-day period.⁴

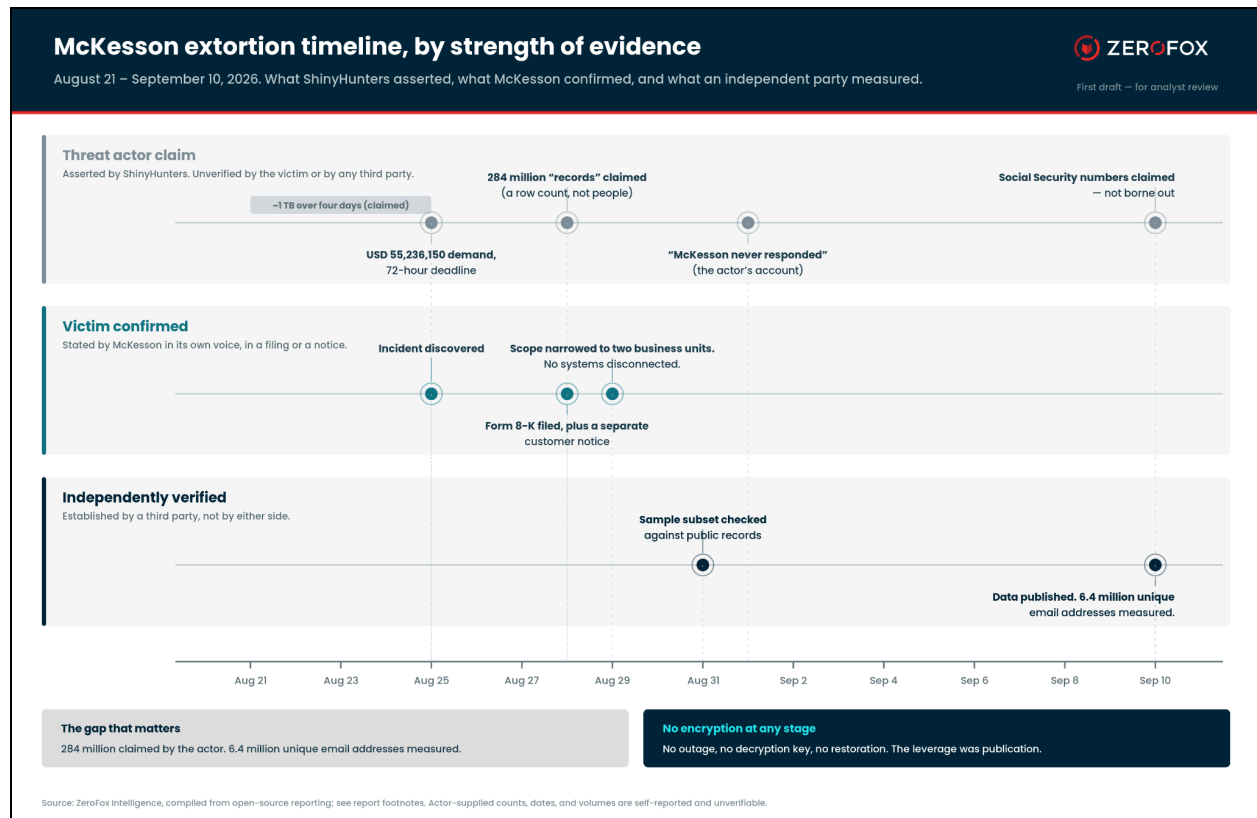
Neither the public disclosures nor the ShinyHunters claim mentioned ransomware or encryption, making it very likely the group did not encrypt McKesson data; instead, ShinyHunters very likely extracted the data, issued a ransom demand, and then almost certainly leaked the data when the victim refused to pay.

¹ [hXXps://haveibeenpwned\[.\]com/Breach/McKesson](https://haveibeenpwned.com/Breach/McKesson)

² [hXXps://www.mckesson\[.\]com/about-us/](https://www.mckesson[.]com/about-us/)

³ [hXXps://www.sec\[.\]gov/Archives/edgar/data/927653/000092765326000247/mck-20260825.htm](https://www.sec[.]gov/Archives/edgar/data/927653/000092765326000247/mck-20260825.htm)

⁴ [hXXps://www.bleepingcomputer\[.\]com/news/security/mckesson-discloses-breach-after-shinyhunters-claims-patient-data-theft/](https://www.bleepingcomputer[.]com/news/security/mckesson-discloses-breach-after-shinyhunters-claims-patient-data-theft/)



McKesson extortion timeline by strength of evidence

Source: ZeroFox Intelligence

Notably, ShinyHunters is known to have encryption capability, as the group released the ShinySpId3r encryptor in November 2025.⁵ ZeroFox assesses that the lack of encryption in the McKesson breach was almost certainly intentional and very likely represents a tactical shift by ShinyHunters from double extortion to encryption-less data theft.

Extortion without encryption is not a new tactic, but its use has grown significantly since late 2025. Europol stated that the extortion model "continues shifting from encrypting data to pressuring victims to pay for their data to not be released."⁶ Additionally, the Federal Bureau of Investigation (FBI) has stated that threat actors extort "without relying on traditional ransomware encryption."⁷

⁵ [hXXps://www.bleepingcomputer\[.\]com/news/security/meet-shinyspId3r-new-ransomware-as-a-service-created-by-shinyhunters](https://www.bleepingcomputer.com/news/security/meet-shinyspId3r-new-ransomware-as-a-service-created-by-shinyhunters)

⁶ [hXXps://www.europol.europa\[.\]eu/cms/sites/default/files/documents/IOCTA-2026.pdf](https://www.europol.europa[.]eu/cms/sites/default/files/documents/IOCTA-2026.pdf)

⁷ [hXXps://www.ic3\[.\]gov/CSA/2026/260526.pdf](https://www.ic3[.]gov/CSA/2026/260526.pdf)

In recent years, observable ransoms paid by encryption victims have been declining; blockchain analysis shows a traced ransom payment rate of 28 percent in 2025, compared to more than 78 percent in 2022.⁸ This reduction has very likely made the costly infrastructure required to run an encryption-based ransomware-as-a-service (RaaS) operation less profitable.

- Encryption has not declined, with more than 50 percent of R&DE incidents involving encryption.⁹ Thus, it is almost certain that encryption-less data extortion is an additional tactic rather than a substitutive one.

The strongest driver of the continuing shift to encryption-less extortion is almost certainly the collapse of any credible assurance that payment results in deletion and the possibility of threat actors retaining decrypted data after ransom payment and attempting re-extortion later. When the UK National Crime Agency (NCA) disrupted LockBit, the group retained data from previous victims who had paid—suggesting that, even when a ransom is paid, there is no guarantee a victim's data will be deleted.¹⁰

The ShinyHunters data breach of McKesson and the subsequent release of sensitive data almost certainly reflect the continuation of the shift in the R&DE ecosystem from encryption-based attacks to “encryption optional” data extortion. While encryption will likely remain the most common attack for the remainder of 2026, the share of R&DE incidents involving encryption will very likely decrease over the next 12 months in favor of encryption-less data extortion.

⁸ [hXXps://www.chainalysis\[.\]com/blog/crypto-ransomware-2026/](https://www.chainalysis.com/blog/crypto-ransomware-2026/)

⁹ [hXXps://www.sophos\[.\]com/en-us/blog/sophos-state-of-ransomware-2026](https://www.sophos[.]com/en-us/blog/sophos-state-of-ransomware-2026)

¹⁰ [hXXps://www.nationalcrimeagency\[.\]gov\[.\]uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos](https://www.nationalcrimeagency[.]gov[.]uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos)

| 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%