



| Flash |

Emerging Threat Actor Targets Data Backups

F-2026-09-29a

Classification: TLP:CLEAR

Criticality: Moderate

Intelligence Requirements: Data Extortion, Threat Actor, Dark Web

September 29, 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 September 29, 2026**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

| Flash | Emerging Threat Actor Targets Data Backups

| Key Findings

- On September 21, 2026, ZeroFox observed a new data leak site attributed to the threat actor "n0n". By the next day, the group had already claimed over a dozen victims on the Tor-hosted site. During its short operational life, n0n has attacked across nearly all business sectors, with technology and professional services combined accounting for 46 percent of its targeting activity.
- What sets n0n apart from other recently launched threat collectives is its threat to encrypt or delete data backups. In recent months, ZeroFox has reported on an increase in the number of ransomware and digital extortion (R&DE) incidents eschewing the encryption model commonly seen in traditional ransomware attacks in favor of encryption-free data extortion.
- The combination of improved data backups and reduced ransom payments has likely created a trajectory in the R&DE landscape that trends toward less encryption and more data extortion. Further, it is unclear whether n0n is able to access victim data backups.
- With a sharp reduction in paid ransoms over the past several years, threat actors will very likely continue to deploy new techniques in an effort to increase profits

and decrease reliance on expensive infrastructure. It is almost certain that further tactical experiments will continue over the next six to 12 months.

| Details

On September 21, 2026, ZeroFox observed a new data leak site attributed to the threat actor n0n. By the next day, the group had already claimed over a dozen victims on the Tor-hosted site.¹

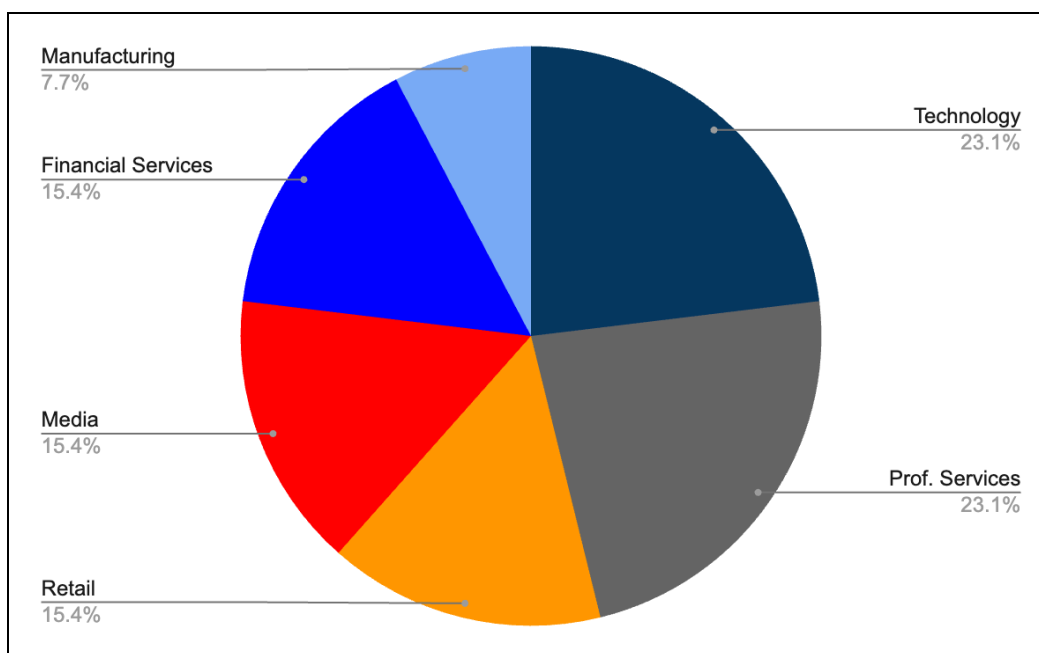
The actor likely achieved initial access through credentials stolen via third-party infostealer malware. The stolen credentials are then used to access corporate networks; privileges are then escalated to allow access to administrative tools in order to manipulate and stage data before encrypting and making ransom demands.²

- During its short operational life, n0n has attacked across nearly all business sectors, with technology and professional services combined accounting for 46 percent of its targeting activity.

What sets n0n apart from other recently launched threat collectives is its threat to encrypt or delete data backups. In recent months, ZeroFox has reported on an increase in the number of R&DE incidents eschewing the encryption commonly seen in traditional ransomware attacks in favor of encryption-free data extortion. This shift across the R&DE landscape has very likely been influenced by an improvement in data backup infrastructure by potential victims.

¹ [hXXps://www.scworld\[.\]com/brief/new-ransomware-group-n0n-escalates-threats-by-targeting-backups](https://www.scworld[.]com/brief/new-ransomware-group-n0n-escalates-threats-by-targeting-backups)

² [hXXps://www.infosecurity-magazine\[.\]com/news/ransomware-gang-uses-backup/](https://www.infosecurity-magazine[.]com/news/ransomware-gang-uses-backup/)



n0n attacks by business sector

Source: ZeroFox Intelligence

Additionally, 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 2022.³ 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; more than 50 percent of R&DE incidents still involve encryption.⁴ Thus, it is almost certain that encryption-less data extortion is an additional technique rather than a substitutive one.

The combination of improved data backups and reduced ransom payments has likely created a trajectory in the R&DE landscape that trends toward less encryption and more data extortion. Further, it is unclear whether n0n is able to access victim data backups. Potential victims—especially in frequently targeted sectors such as technology and professional services—likely separate data backups from their primary networks,

³ <https://www.chainalysis.com/blog/crypto-ransomware-2026/>

⁴ <https://www.sophos.com/en-us/blog/sophos-state-of-ransomware-2026>

resulting in a roughly even chance that a threat actor can access and encrypt the data in a single attack.

Threats against victim backups would almost certainly demonstrate that threat actors are seeking ways to monetize their activity in an environment where victims are paying ransoms less often. With a sharp reduction in paid ransoms over the past several years, threat actors will very likely continue to deploy new techniques in an effort to increase profits and decrease reliance on expensive infrastructure. It is almost certain that further tactical experiments will continue over the next six to 12 months.

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%