ZEROFOX INTELLIGENCE

Flash

DeadLock's Ransomware Leak Site Lists over 80 Victims

F-2026-06-26a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Ransomware, Extortion, Cryptocurrency

June 26, 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 4:00 AM (EDT) on June 25, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | DeadLock's Ransomware Leak Site Lists over 80 Victims

| Key Findings

- On June 16, 2026, ZeroFox observed a ransomware leak site titled "DeadLock" that listed roughly 80 victims.
- About 57 percent of the total observed claimed victims are located in the Europe-Russia region, while Asia-Pacific (APAC), North America, South America, and the Middle East and Africa collectively account for the remainder of the listings.
- ZeroFox assesses that the group is very likely primarily focused on extracting ransom amounts from the listed entities rather than establishing its presence in the cybercrime ecosystem.
- ZeroFox assesses that the group's widespread regional and industry targeting, availability of data download links, and reported campaign techniques indicate a roughly even chance that many listed victims were legitimately impacted.

Details

On June 16, 2026, ZeroFox observed a ransomware leak site titled DeadLock that listed roughly 80 victims. The clearnet domain for the leak site (hXXps://deadlock.liveblog365[.]com) is unavailable at the time of reporting. Considering the sheer volume of victims listed in a relatively short span of time, ZeroFox assesses the collection is likely a list of all the entities the operation has targeted since its founding. The leak site is very likely associated with the ransomware group of the same name.

- DeadLock's leak site currently includes names of the targets and associated extortion claims but does not provide sufficient evidence to prove the intrusions.
- A link to download allegedly leaked data for some of the older targets was added to the site but has since become inaccessible.
- The leak site displayed a message asking visitors to download an HTML version of the page, citing frequent deletion—a common occurrence for leak sites hosted on the clearnet.

Sample listing from DeadLock's leak site
Source: ZeroFox Intelligence

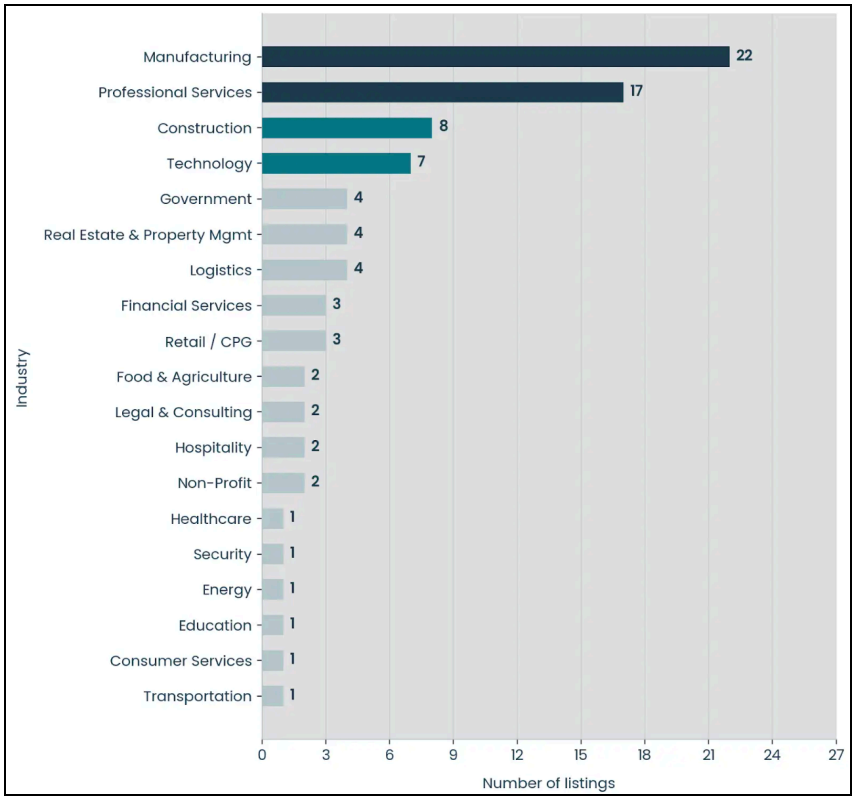
Cybersecurity researchers first observed the DeadLock ransomware operation in mid-2025. The operation is known to use smart contracts on Polygon, a blockchain platform that operates in conjunction with the Ethereum blockchain. Additionally, it appears to rely heavily on the privacy-focused Session messaging platform, along with AnyDesk for remote access and persistence during intrusions.[1]

- DeadLock's reported encryption mechanism—which involves leveraging custom cryptographic implementations rather than standard Windows Application Programming Interfaces (APIs)—likely enables the group to efficiently encrypt data while bypassing standard detection techniques.
- Additionally, the use of blockchain-based infrastructure likely improves the group's resilience against takedown efforts.
- In one of its ransom notes, DeadLock claimed to use "military-grade encryption"—a common claim by threat actors, almost certainly a psychological pressure tactic to convince victims decryption is impossible without a private key. The note also included a unique Session ID for the victim to make contact and discuss their ransom payment.

About 57 percent of the total claimed victims are located in the Europe-Russia region, while APAC, North America, South America, and the Middle East and Africa account for the remainder of the listings. The claimed victims span multiple sectors, although manufacturing organizations are the majority.

- The manufacturing industry remains a popular and lucrative target for ransomware actors, almost certainly due to its dependence on operational continuity, interconnected supply chains, and limited ability to withstand prolonged disruptions.

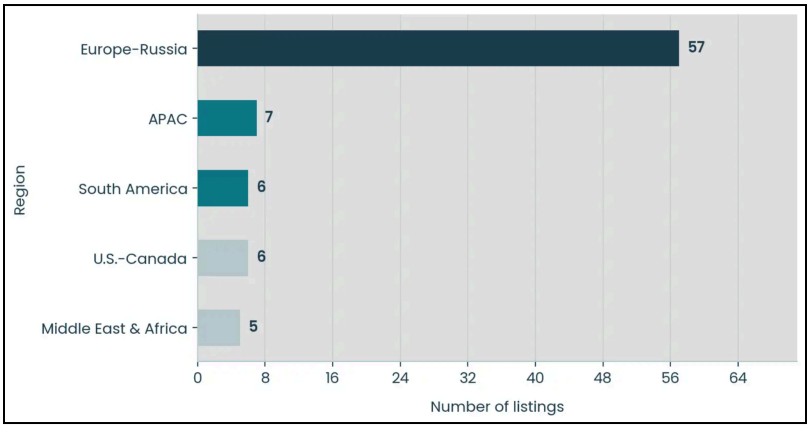
[1] hXXps://www.bankinfosecurity[.]com/deadlock-ransomware-group-utilizes-polygon-smart-contracts-a-30518



DeadLock's victims categorized by industry

Source: ZeroFox Intelligence

- DeadLock's victim distribution suggests that the group is prioritizing targets in Europe, likely influenced by access opportunities and regional targeting preferences.

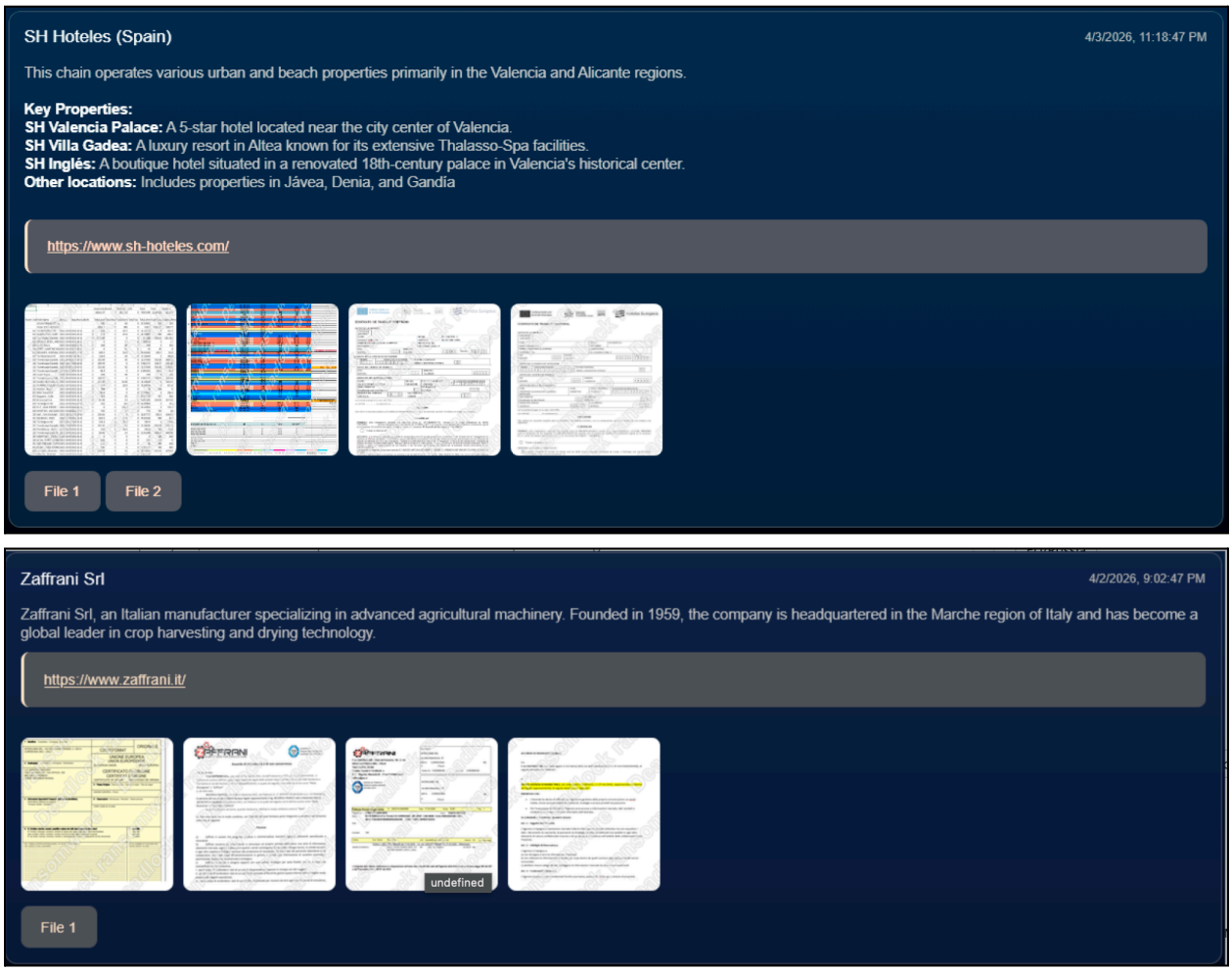


DeadLock's victims categorized by region

Source: ZeroFox Intelligence

Some of the listings on the DeadLock leak site include links to download allegedly stolen data from the targeted entities, including the websites of Spanish hotel chain SH Hoteles and Italian agricultural machinery manufacturer Zaffrani. It is likely the actors released the data after failed negotiations or a complete refusal to pay the ransom amount.

- Despite the high volume of listings, it is likely the listed victims are from older ransomware and extortion campaigns conducted by the same group.
- It is very likely the group is primarily focused on extracting ransom amounts from the listed entities rather than establishing its presence in the cybercrime ecosystem.



Listings for SH Hoteles and Zaffrani, with links to download allegedly stolen files

Source: ZeroFox Intelligence

The links to download allegedly stolen data from some of the entities, as well as the campaign's seemingly widespread regional and industry targeting and its reported techniques, indicate a roughly even chance that at least some, if not all, of the listed victims were legitimately impacted.

It is likely that the group will reach out to the listed entities—excluding the ones for which data download links have been shared—for ransom negotiations. If the negotiations fall through, the group is very likely to leak the allegedly stolen data.

- As the leak site is hosted on the clearnet, it is likely to face removal risk on a frequent basis, leading to the high volume of listings in a short time span.

As of writing, the threat from DeadLock ransomware is likely low. There is not enough evidence to suggest that the group has targeted a supply chain; hence, the alleged intrusions are unlikely to have impacted organizations other than the ones listed on the leak site. However, the group is likely to evolve its tactics, techniques, and procedures (TTPs) to further scale up its operations and target other entities in the future.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.

| 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%