



| Flash |

Data Breach in Berlin Weeks Ahead of Election

F-2026-09-18b

Classification: TLP:CLEAR

Criticality: Moderate

Intelligence Requirements: Dark Web, Threat Actor, Geopolitics

September 18, 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 18, 2026**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

| Flash | Data Breach in Berlin Weeks Ahead of Election

| Key Findings

- On August 28, 2026, threat actor “Rhysida” advertised the sale of 5.79 TB of data allegedly exfiltrated from the city government of Berlin, Germany. The breach was confirmed by the government of Berlin on August 14, 2026, while the attack itself very likely occurred between August 7–12, 2026.
- Rhysida claims the data includes violations of the General Data Protection Regulation (GDPR), the European Union (EU)’s comprehensive data law that governs the safekeeping of the personal data of EU citizens or residents held digitally by organizations. The threat actor very likely used alleged GDPR violations as leverage to persuade Berlin to pay the ransom.
- Berlin’s subsequent refusal to pay is consistent with guidance from the German federal cybersecurity agency; it likely reflects a government priority to show resolve against cybercrime in the lead-up Berlin State elections to be held on September 20, 2026, for both a new state parliament and local district councils.
- ZeroFox assesses that, as further elections across Europe draw near over the next six to 12 months, threat actors will almost certainly seek to influence outcomes by conducting timed operations likely intended to sow distrust in government institutions.

| Details

On August 28, 2026, threat actor Rhysida advertised the sale of 5.79 TB of data exfiltrated from the city government of Berlin, Germany. The offering was posted on Rhysida's dark web leak site for 30 Bitcoin (roughly USD 75,000 at the time of writing). The threat actor also reportedly targeted data from the German Senate's Department for Mobility, Transport, Climate Protection and the Environment.¹

The breach was confirmed by the government of Berlin on August 14, 2026; the attack itself very likely occurred between August 7–12, 2026, according to the Berlin State government.² Rhysida claims the data exfiltrated includes:

- Government, legal, financial, contractual, HR, infrastructure, health, and mapping records
- Thousands of names, email addresses, and phone numbers, as well as 148 international bank account numbers
- Plaintext credentials, database accounts, payment-system data, password vaults, and credentials belonging to senior officials
- Personnel files, payroll information, administrative-offense records, email archives, SQL database dumps, identity documents, and banking information
- Documents related to disciplinary proceedings and other named cases
- Allegedly classified or sensitive government material, including Bundesrat committee records and information about handling classified documents
- Critical-infrastructure security assessments concerning Berlin's water supply
- More than 3,200 documents marked as nondisclosure agreements³

Rhysida further claims the data includes violations of the GDPR, the EU's comprehensive data law that governs the safekeeping of the personal data of EU citizens or residents held digitally by organizations.⁴ The threat actor very likely used alleged GDPR violations as leverage to persuade Berlin to pay the ransom. However, the government of the

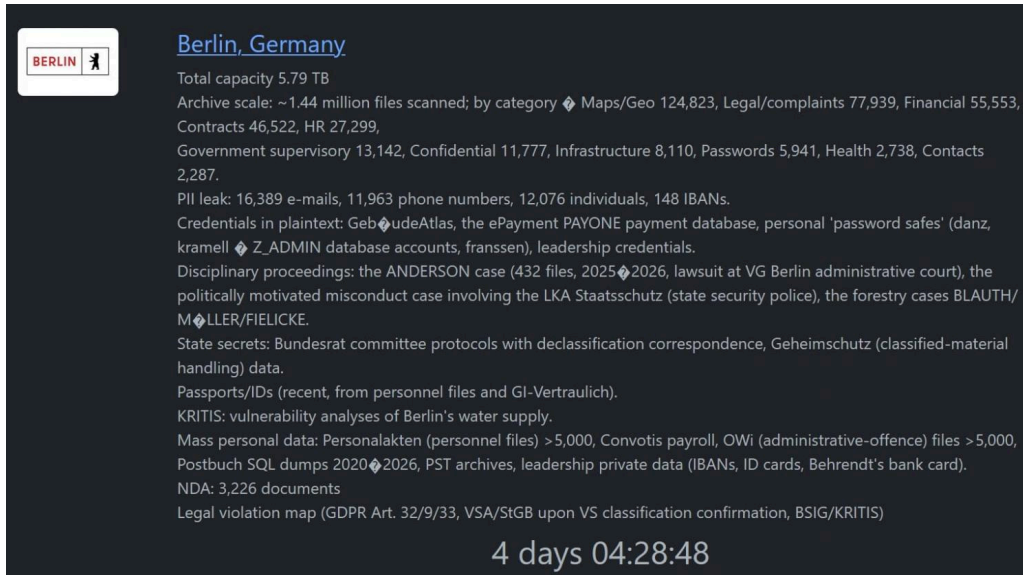
¹ [hXXps://www.bleepingcomputer\[.\]com/news/security/berlin-confirms-data-theft-after-rhysida-ransomware-attack-claims/](https://www.bleepingcomputer.com/news/security/berlin-confirms-data-theft-after-rhysida-ransomware-attack-claims/)

² *Ibid.*

³ *Ibid.*

⁴ [hXXps://securityaffairs\[.\]com/198064/cyber-crime/rhysida-ransomware-group-targets-berlin-government-ahead-of-vote.html](https://securityaffairs.com/198064/cyber-crime/rhysida-ransomware-group-targets-berlin-government-ahead-of-vote.html)

German capital refused to pay,⁵ almost certainly leading to the subsequent sale advertisement.



Berlin, Germany

Total capacity 5.79 TB

Archive scale: ~1.44 million files scanned; by category ♦ Maps/Geo 124,823, Legal/complaints 77,939, Financial 55,553, Contracts 46,522, HR 27,299,

Government supervisory 13,142, Confidential 11,777, Infrastructure 8,110, Passwords 5,941, Health 2,738, Contacts 2,287.

PII leak: 16,389 e-mails, 11,963 phone numbers, 12,076 individuals, 148 IBANs.

Credentials in plaintext: Geb♦udeAtlas, the ePayment PAYONE payment database, personal 'password safes' (danz, kramell ♦ Z_ADMIN database accounts, franssen), leadership credentials.

Disciplinary proceedings: the ANDERSON case (432 files, 2025♦2026, lawsuit at VG Berlin administrative court), the politically motivated misconduct case involving the LKA Staatsschutz (state security police), the forestry cases BLAUTH/M♦LLER/FIELICKE.

State secrets: Bundesrat committee protocols with declassification correspondence, Geheimschutz (classified-material handling) data.

Passports/IDs (recent, from personnel files and GI-Vertraulich).

KRITIS: vulnerability analyses of Berlin's water supply.

Mass personal data: Personalakten (personnel files) >5,000, Convotis payroll, OWi (administrative-offence) files >5,000, Postbuch SQL dumps 2020♦2026, PST archives, leadership private data (IBANs, ID cards, Behrendt's bank card).

NDA: 3,226 documents

Legal violation map (GDPR Art. 32/9/33, VSA/StGB upon VS classification confirmation, BSI/KRITIS)

4 days 04:28:48

Rhysida's initial announcement of Berlin breach

Source: ZeroFox Intelligence

Berlin's refusal to pay is consistent with guidance from the German federal cybersecurity agency⁶ and comes less than a month before the Berlin State elections on September 20, 2026, when both a new state parliament and local district councils will be elected to serve five-year terms.⁷ Berlin's refusal to pay the ransom was very likely influenced by the upcoming elections, highlighting that governments are likely to show resolve against cybercrime in the lead-up to important elections.

Rhysida's timing is unlikely to be a coincidence. There is a roughly even chance the threat actor timed this operation, and the subsequent leak of data, to influence the Berlin State elections. ZeroFox assesses that, as further elections draw near across Europe over the next six to 12 months, threat actors will almost certainly seek to influence outcomes by conducting timed operations likely intended to sow distrust in government institutions.

⁵ *Ibid.*

⁶ [hXXps://tech-insider\[.\]org/berlin-confirms-data-theft-rhysida-ransomware-2026/](https://tech-insider[.]org/berlin-confirms-data-theft-rhysida-ransomware-2026/)

⁷ [hXXps://www.rbb24\[.\]de/politik/berlin-wahl-2026/beitraege/faq-englisch-berlin-elections-state-parliament-district-councils.html](https://www.rbb24[.]de/politik/berlin-wahl-2026/beitraege/faq-englisch-berlin-elections-state-parliament-district-councils.html)

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%