Continue

Free of leaks

DDoSecrets, a non-profit organization that hosts leaked and hacked data in the public interest, has launched its sixth-anniversary celebration by making millions of files searchable on its website. The new interface, known as the Library of Leaks, already contains over 10 million files and is expected to continue expanding. The project was officially launched at LibraryOfLeaks.org on Tuesday, with DDoSecrets describing it as “the world's largest public collection of previously secret information.” The organization said the tool already holds millions of documents from several leaks and will continue to add more data daily. Searchable files include those from the Israeli Ministry of Justice, Metropolitan Police Department, FBI, and WikiLeaks. The library is also hosting emails from former Secretary of State Hillary Clinton. As part of its anniversary celebration, DDoSecrets has released two new datasets: one from the Kazakhstan Ministry of Energy containing tens of thousands of documents, presentations, and internal materials obtained by hackers in 2022. Another dataset features approximately 75 videos from far-right podcaster Andrew Tate's "The War Room," a secretive society that offers membership for $8,000 a year. DDoSecrets will still be the primary source for downloading raw data, but the Library of Leaks search engine makes it easier to access much of the information. The organization said the tool puts the most significant leaks of the last 20 years in one place and empowers research into governments and corporations that shape our lives. Access to millions of documents from dozens of leaks, with new additions daily, has been restored through DDoSecrets' initiative, mirroring its original goal of providing a public resource for leaked data. This came after their first search engine, Hunter Memorial Library, was seized by German police in 2020 at the behest of U.S. law enforcement. Collaborations with Flokinet and Investigative Data, as well as public donations, have made The Library of Leaks possible. To ensure sensitive data remains secure, DDoSecrets has introduced a "library card" system for researchers and journalists who need access to their Reserved collection. This section contains personally identifiable information (PII), requiring stricter access controls to protect privacy. Access will continue to be vetted, ensuring that those accessing the Reserved collection demonstrate a commitment to protecting individual privacy. In addition, DDoSecrets is implementing multi-factor authentication through physical access devices, a response to recent security incidents involving leaks from the Reserved section. The organization emphasizes the importance of these measures, stating that they can endanger sources and the public. Despite this, DDoSecrets aims to make the new system accessible to all who need it, urging those unable to afford subscriptions to contact them. The rise in AI use has led to an increase in secret sprawl, with companies of various sizes and sectors falling victim to leaks involving AI API tokens. The wide adoption of AI tools by both tech and non-tech individuals has diversified the sources of these leaks. Recent incidents have shown that no company seems immune to this risk, including xAI, the company behind Grok AI assistant, which fell victim to a leak in March 2025. GitGuardian's secret detection platform continuously scans public GitHub repositories for new secrets, sending automated alerts to commit authors through its Good Samaritan Program. On March 2nd, 2025, this system discovered an xAI API key in an .env file, alerting the commit author to the incident. The unique aspect of this leak was that it was linked to a committer's email address hosted under the x.ai domain. Two months after initially discovering the leak, Philippe Caturegli, an independent security researcher, stumbled upon an xAI API key in a public repository and notified GitGuardian. This led to further investigation, revealing that the API key was still valid and granted access to unreleased models. We decided not to investigate further but instead formally notify x of the breach via responsible disclosure. The private models potentially contained sensitive information about X's intellectual property. We prepared a detailed disclosure email with information on the leak source, affected keys, and accounts, and then encountered an issue - xAI doesn't have a publicly exposed security.txt file, which is an industry standard for providing security contact information. We had to manually search for alternative contact methods, eventually finding the safety@x.ai email address. After sending the disclosure email, we received a response from xAI 12 hours later, asking us to submit the report through their Bug Bounty Program on HackerOne. This would delay the remediation process, and we chose not to participate in the bug bounty program, instead opting for direct communication with xAI's team. Secret leaks happen to every company without distinction, and we can't blame xAI or its developers for that. Every company should be prepared to receive security alerts for such incidents. The xAI case illustrates some common misconceptions and bad practices when it comes to responsible disclosure handling: no easily identifiable security contact, using a bug bounty program to replace an appropriate CSIRT team, and no transparent communication to researchers without updates about remediations. To be better prepared, have a team identified to handle disclosure inbound, give public information about security contacts, fine-tune your bug bounty scopes and policies, and follow a transparency-first approach in communications. The Free data leak breach has left millions of customers worried. The sale of the affected database concluded on October 29, with a final bid reaching €175,000. As you navigate the coming months, be aware of potential threats like phishing attacks, identity theft, and fraudulent use of IBANs. To stay protected, change your passwords immediately, implement multi-factor authentication, and review linked devices, apps, and accounts. Additionally, keep software updated regularly and monitor bank transactions closely. CybelAngel's REACT team analyzes and responds to cyber threats by investigating data leaks rapidly. If you're a cybersecurity professional concerned about the rise in Telecom ransoming, get in touch with us for expert assistance. The Telecom industry is a hot target for cyber attacks, and it's crucial to be primed to investigate and remediate incidents. DeHashed offers robust open-source intelligence through its Realtime Feed, providing essential information for risk assessment, threat detection, and protection against fraudulent attacks. The platform aggregates vast amounts of data, including unmodified raw data, breach monitoring, and verified records, to empower users with real-time insights. Key features include: - Real-time data discovery - Deduplicated data - Total records analysis - Incident response time evaluation - Reliance on external sources Pricing plans vary, starting at $0.02 for a 6-hour window, with options for subscription-based models and API access for custom applications. DeHashed aims to make security accessible by offering free services while maintaining comprehensive data coverage and state-of-the-art security measures. Partnerships with law enforcement agencies and Fortune 500 companies underscore its commitment to providing reliable protection solutions.