Unmasking ByteToBreach with KELA Cyber

Published: 2025-11-17 · Archived: 2026-04-05 13:39:15 UTC

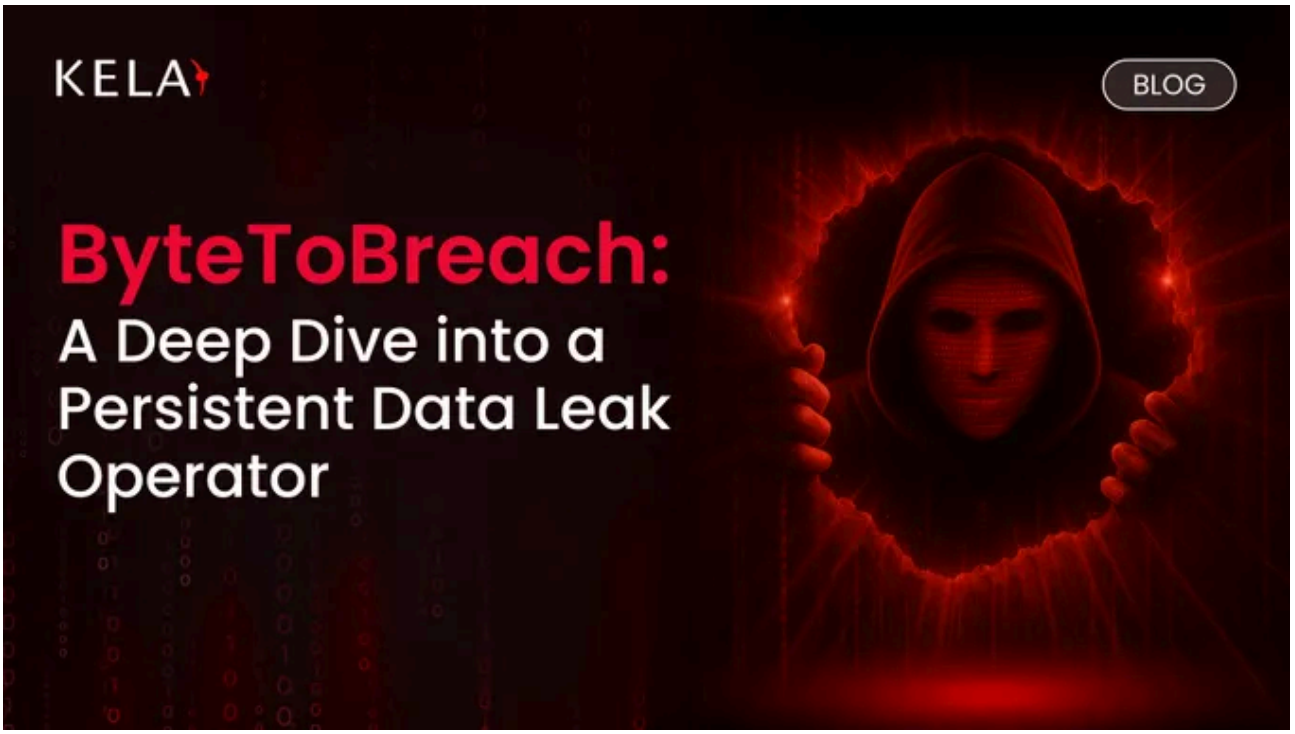
ByteToBreach: A Deep Dive into a Persistent Data Leak Operator

KELA uncovers ByteToBreach, a technically skilled cybercriminal selling sensitive global data from airlines, banks, and governments. This profile reveals his tactics, targets, and online identities across dark web platforms.

KELA

By KELA Cyber Intelligence Center

Published November 17, 2025



KELA's investigation has traced the activity of a prolific cybercriminal operating under the handle ByteToBreach, active since at least June 2025. The actor has run an extensive, cross-platform operation that blends real technical capability with aggressive self promotion and monetization. Operating across DarkForums, Dread, Telegram, and a public WordPress site, the actor has sold and leaked sensitive databases from airlines, banks, universities, government entities, and other high-value targets around the globe.

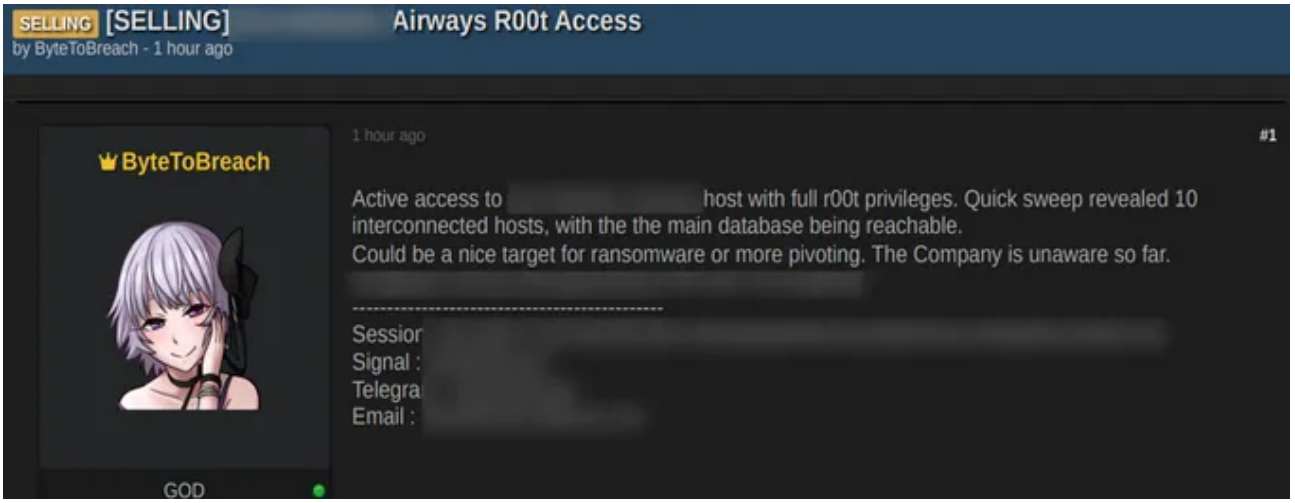
Take note: The full threat actor profile, including exclusive and detailed information not covered in this blog, is available to KELA customers and upon request.

» Get started for free with KELA and strengthen your cybersecurity

Victimology and Impact

The actor's leaks and sales show a wide geographic reach and a preference for high impact targets that attract attention - airline passenger manifests, banking employee records, healthcare databases, and government-related files. Several incidents included datasets that were later corroborated by affected organizations or contained verifiable technical artifacts, underscoring that many of the actor's claims were not mere bluff. The affected companies span multiple countries, such as Ukraine, Kazakhstan, Cyprus, Poland, Chile, Uzbekistan, the United States, and others.

These compromises have consequences that go beyond immediate financial loss: exposed personal data increases risks of identity theft and fraud for affected individuals, leaked internal documents can undermine trust in institutions, and access to corporate systems can enable follow-on attacks such as ransomware or supply-chain exploitation.



» Understand how threat actors breach and exploit your data

Methods and Tradecraft

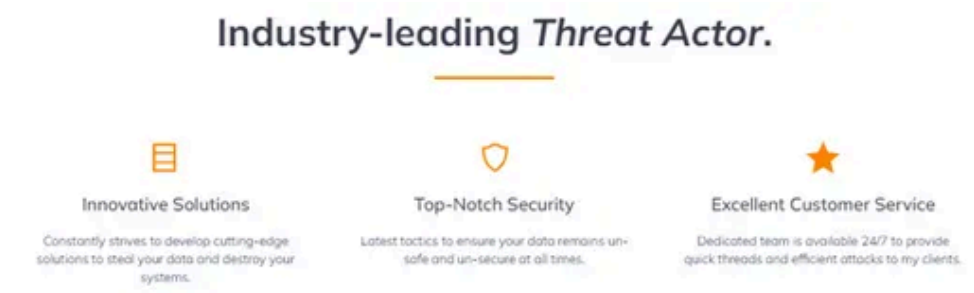
Based on ByteToBreach posts, he uses a mix of multiple technical approaches: Exploiting known vulnerabilities in cloud and corporate infrastructure, reusing stolen credentials harvested from infostealers and phishing, and at times resorting to brute force or misconfiguration based access to gain footholds. Once inside, the focus is data exfiltration - employee records, databases, backups, and sensitive documents that are later sold or leaked publicly to prove claims.

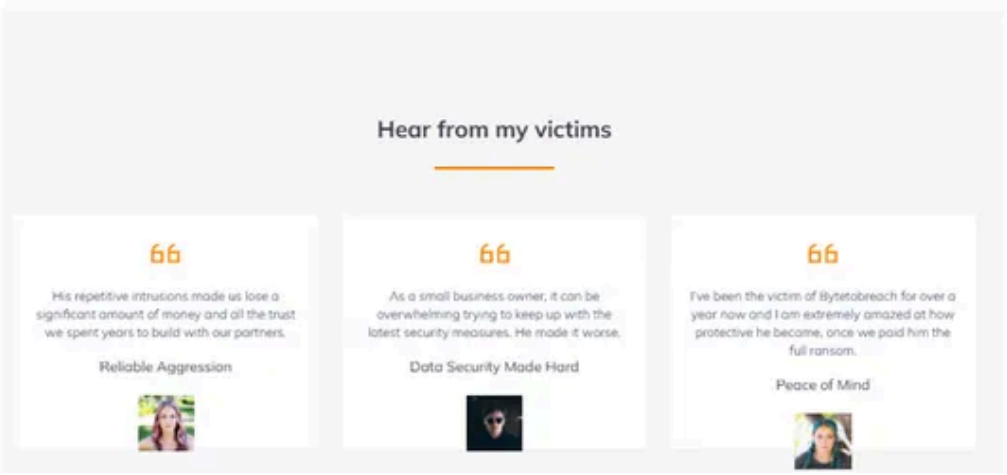
ByteToBreach frequently stated that he had tried to contact victim organizations, asserting that "innocent people are the victims, not the governments. Remember that", and demanded that companies take responsibility for protecting their customers. These comments appeared most prominently in connection with the Uzbekistan Airlines incident, where he continued releasing large amounts of passport data to back his claims. Most of his leaks appeared legitimate and credible, with some organizations, such as a bank in Poland, acknowledging the breaches. In addition to selling data, he also sought technical services, such as offering $100 per hash for cracking.

» Learn how to prevent phishing attacks before they catch you

OSINT Traces

ByteToBreach established a website in August 2025 under the name “Pentesting Ltd”, built on WordPress. The site was designed to resemble a professional service provider, prominently displaying logos of the companies he claimed to have hacked as “clients”. Large banners on the site featured phrases such as “Let Me Harm Your Data”, “Compromise your servers with the most powerful intrusion”, and “Industry-leading Threat Actor”. The website also included fabricated “statistics,” highlighting “angry clients” and “stolen data”, and concluded with contact information while explicitly warning not to reach out if the visitor is a terrorist or a pedophile.

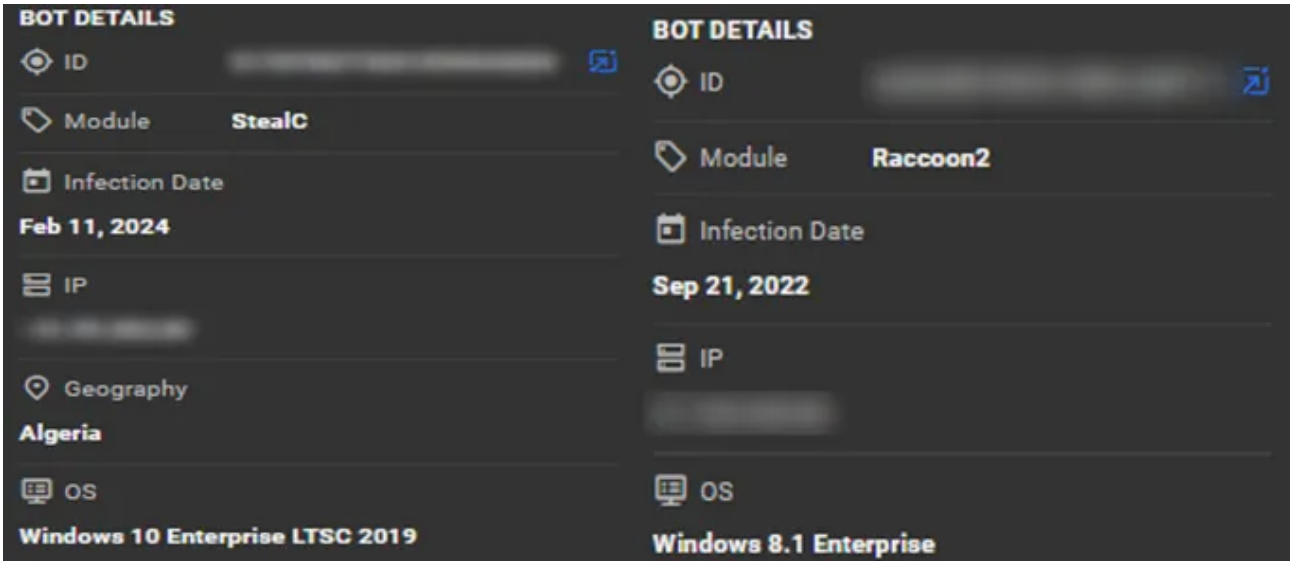




While investigating the actor's posts, KELA observed that he communicated through multiple channels, including email domains such as ProtonMail, Tuta, and Gmail, as well as Telegram (@ByteToBreach, with former names such as "CvHNWwEG" and "inesslopez"), Signal, and Session, occasionally sharing or selling data via Google Drive links. Using these contacts, KELA linked him to the Dread platform, where he registered in June 2025, mainly reposting content from DarkForum while advising users on hacking and accessing leaked data. He also maintained a Pastebin account under the same username to publicly publish some of his leaks.

Using the unique Session ID the actor is using, KELA identified another profile the actor used by another DarkForum user that was active in June 2025, who mainly commented on other users' threads and leaked databases from Singapore companies. Contact emails linked to this account were also associated with ProtonMail, Gmail, and Tuta domains. In late June 2025, after one user accused him of scamming 500 euros, the actor went dark. Posts under this username also indicate he was registered on Dread as well.

KELA's datalake analysis of the new username revealed two bots infostealer infected machines, both originating from Algeria and containing these usernames as logins for multiple services including ProtonMail, Instagram, and TransferWise. One bot had been infected with Raccoon in September 2022, and the other with StealC in February 2024. While the bots did not contain evidence of hacking forum activity, some direct connections to ByteToBreach were identified: the former Telegram username "inesslopez" appeared in the bot data, and a phone number appeared in this bot is directly tied to the Telegram account of ByteToBreach.



The two bots from KELA's platform

» Find out why your organization needs cyber threat intelligence

Conclusion

ByteToBreach has demonstrated credible activity, with many of his claimed breaches across various sectors appearing legitimate. His claims were often supported by verifiable proof, such as database access and other technical artifacts. The actor exemplifies a modern underground operator who blends legitimate technical skill with criminal intent and a marketing-first approach to selling stolen data. The technical and behavioral patterns are clear: this is an adaptable, opportunistic threat.

OSINT and technical investigations show consistent use of multiple aliases across emails, messaging platforms, and session identifiers, linking these online identities to a single actor.

» Looking for the solution? Look no further than KELA
