THREAT HUNTER RESEARCH

H1 2026 Enterprise Brand External Risk Report

A half-year view of the channels, assets, and tactics behind brand impersonation, phishing, counterfeit distribution, and related external risk.

Original publication: 2026-07-30
Research team: Threat Hunter Research Team
Source report: 29 pages

Read instructions

This text version is reconstructed based on the 29-page original PDF and the full text of the published web page, retaining the report narrative, chapters, tables, and original charts; the cover, duplicate table of contents, and purely decorative pages are not repeated.

Following the release of the "Research Report on Internet Cybercrime Ecosystem in the First Half of 2026", Threat Hunter further focused their observation perspective beyond the boundaries of corporate brands and officially released the "Research Report on External Risks of Corporate Brands in the First Half of 2026".

In the first half of 2026, corporate brand protection is undergoing a profound transformation, shifting from disposing of single counterfeit assets to protecting trusted connections between companies and users. Risks such as data leakage, identity fraud, channel interception and public disclosure are jointly affecting brand identity, official channels, customer relations and public reputation from different locations. We sorted out five core judgments around the four sections of brand external risk panorama, risk formation mechanism, key industry differences and typical cases. Together, these five judgments present a set of interrelated risk changes: brand protection is no longer just about detecting and removing counterfeit assets, but also requires identifying information exposure, channel abuse and their ongoing impact on user trust.

core summary

- Brand protection is shifting from dealing with single counterfeit assets to protecting trusted connections between enterprises and users, involving four aspects: brand identity, official channels, customer relations and public reputation; data, channel and content risks that occur outside the boundaries of the enterprise may also continue to damage brand trust.
- The total number of data breach incidents increased slightly, but major risks rose faster and were further concentrated on the dark web. A total of 23,645 data leakage incidents were confirmed in the first half of 2026, an increase of 6.98% compared with the second half of 2025; including 542 major incidents, an increase of 22.90%. The proportion of the dark web in major incidents increased from 76.64% to 95.02%, and it has become the main external channel for the public disclosure and dissemination of major data risks.
- Search and counterfeit websites are the most concentrated entry points for brand channel abuse, and users may be blocked before finding official services. A total of 45,321 phishing, counterfeiting and brand abuse incidents were recorded in the first half of the year, of which SEO pollution accounted for 45.73% and counterfeit websites accounted for 29.56%. Search results, content platforms, social media, customer service hotlines, applications and download channels are forming a multi-entry parallel risk network.
- Combining real business information with fake identities and unofficial channels will significantly enhance the credibility of the fraud. Leaked loan, order, refund or collection information can help risk subjects restore the user's business background, and then complete the contact through fake text messages, customer service, high imitation pages or dynamic QR codes, both of which jointly strengthen the "official" illusion.
- Different industries face significantly different external risk structures and require differentiated protection strategies. Finance and lending are both under pressure from customer data exposure and identity theft; e-commerce risks are mainly concentrated in marketing, transactions and after-sales portals; the manufacturing and retail industries are more

susceptible to the public disclosure of major data events and business continuity; the gaming industry is dominated by counterfeit social media, private servers, account transactions and product infringement.

Chapter 1 Two types of core risk aspects of brand external risks

Risks external to the enterprise are not concentrated on a single phishing page or a single data breach. Data and identities may continue to flow beyond corporate control, and user touchpoints may be dispersed across search, content, social, download and private channels. The core issue facing brand protection is expanding from "whether there are counterfeit assets" to "whether the trusted connection between the enterprise and the user is still identifiable and controllable."

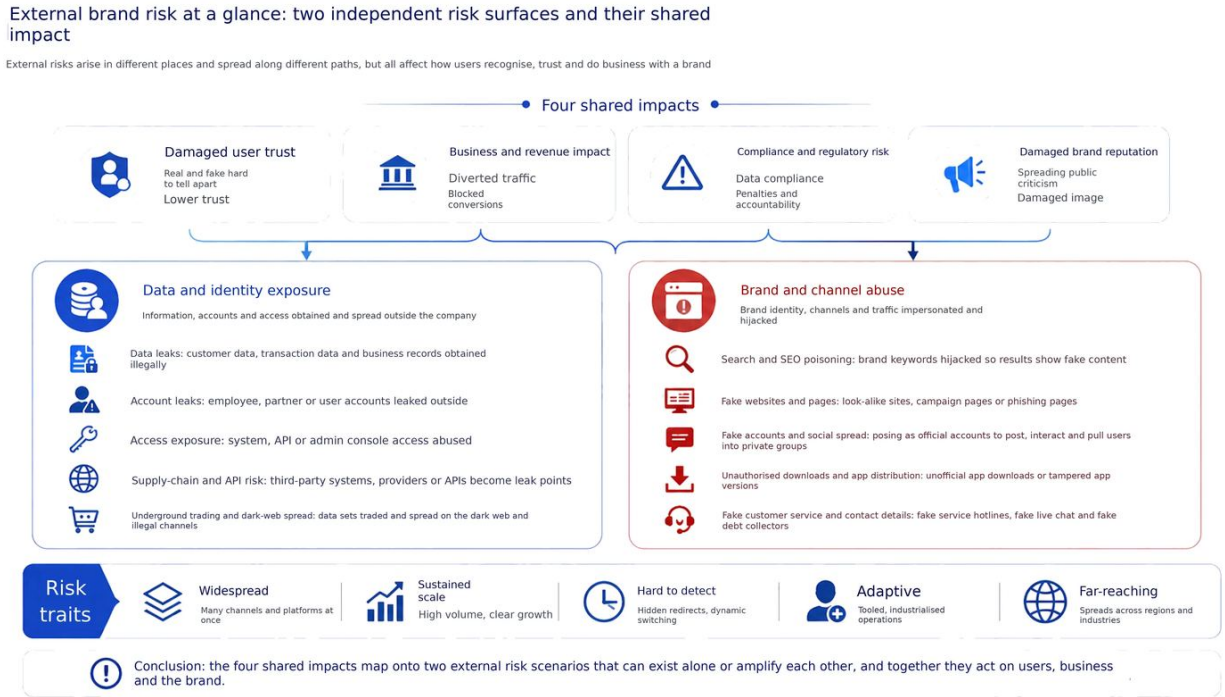
1.1 Brand protection revolves around four categories of objects

Protected asset	Main external risks	Typical impact
Brand identity	Company and product names, logos, domains, apps and official accounts are impersonated	Users cannot tell who provides the service; authorisation and brand order are damaged
Official channels	Search results, websites, service hotlines, download links, content accounts, campaign pages and QR codes are intercepted	Users reach fake contacts, unauthorised downloads or fraud pages before the official service
Customer relationships	Real records of loans, payments, orders, memberships, refunds and collections reach outside channels	Account histories are rebuilt and targets screened, so fake service or collection scripts become more precise
Public reputation	Dark-web disclosures, attack claims, data samples and infringing content spread publicly	Customer doubts, partner reviews, public pressure and business-continuity risk rise

The four assets that brand protection covers, with their main external risks and typical impact

Source: Threat Hunter original report, page 7. Table re-typeset in English from the original.

Focusing on the above four types of protection objects, the external risks faced by enterprises can be summarized into two relatively independent risk areas: exposure of data, identity and permissions, and abuse of brand, channel and traffic. The two can occur independently or overlap each other, jointly affecting customer relationships, user trust and brand reputation.

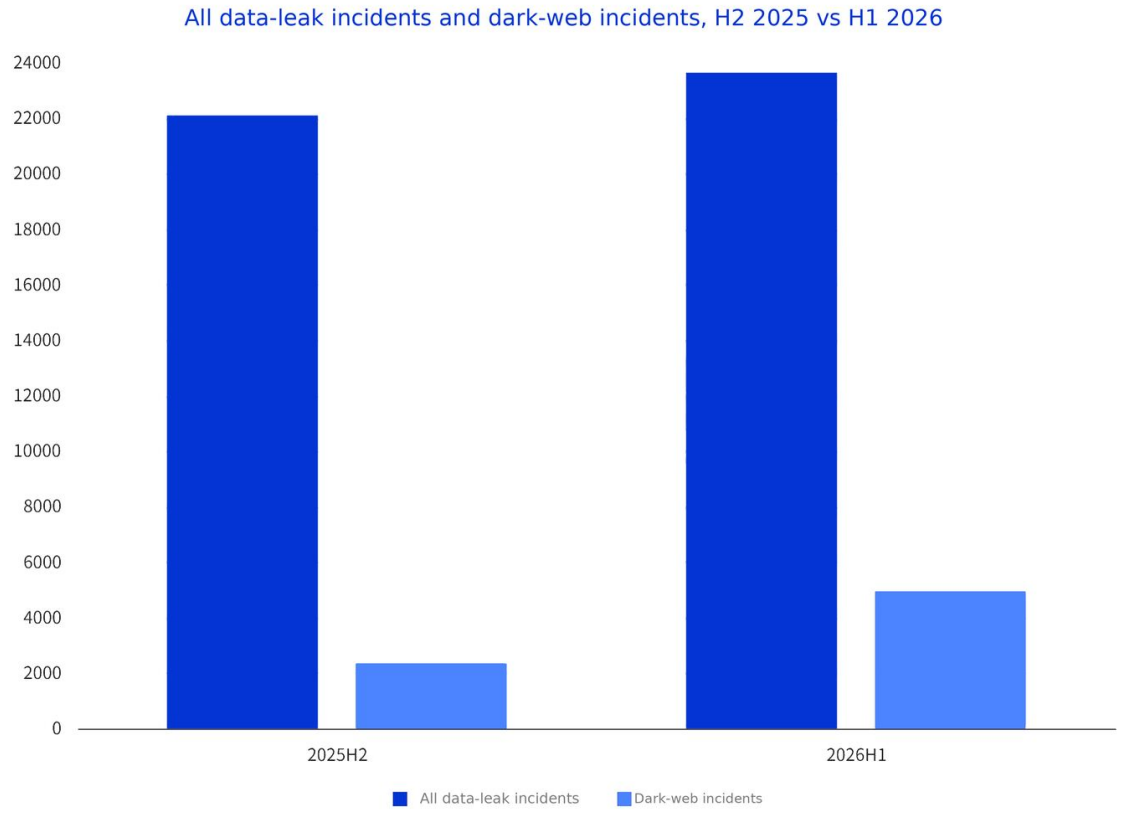


External brand risk at a glance: data and identity exposure, and brand and channel abuse, lead to four shared impacts

Source: Threat Hunter original report, page 7. Original figure with Chinese text replaced by English.

1.2 The total number of data leakage incidents increased slightly, and major risks were concentrated on the dark web.

From January to June 2026, there were a total of 23,645 verified and confirmed valid data leakage incidents, an increase of 6.98% from 22,102 incidents in the second half of 2025. Among them, darknet channel records increased from 2,353 to 4,952, an increase that was significantly higher than the increase in overall incidents.

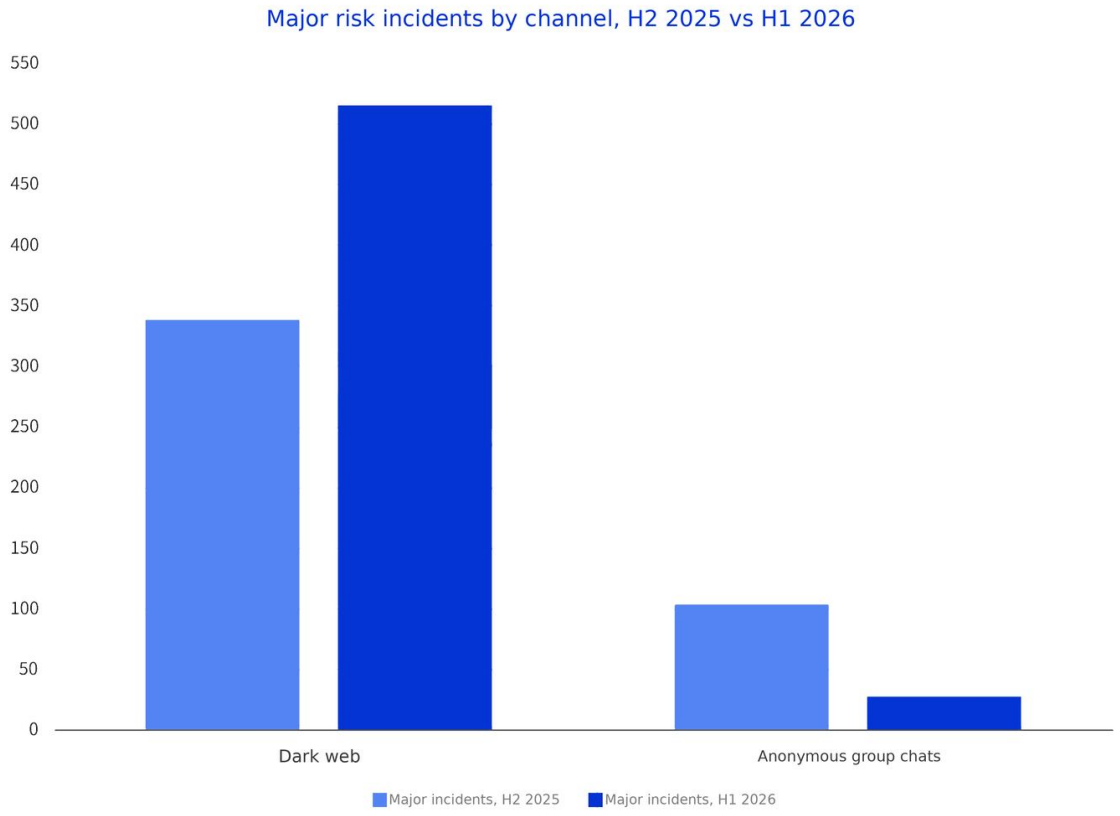


All data-leak incidents and dark-web incidents, H2 2025 vs H1 2026: total incidents rose 6.98% to 23,645 while dark-web incidents grew from 2,353 to 4,952

Source: Threat Hunter original report, page 8. Original figure with Chinese text replaced by English.

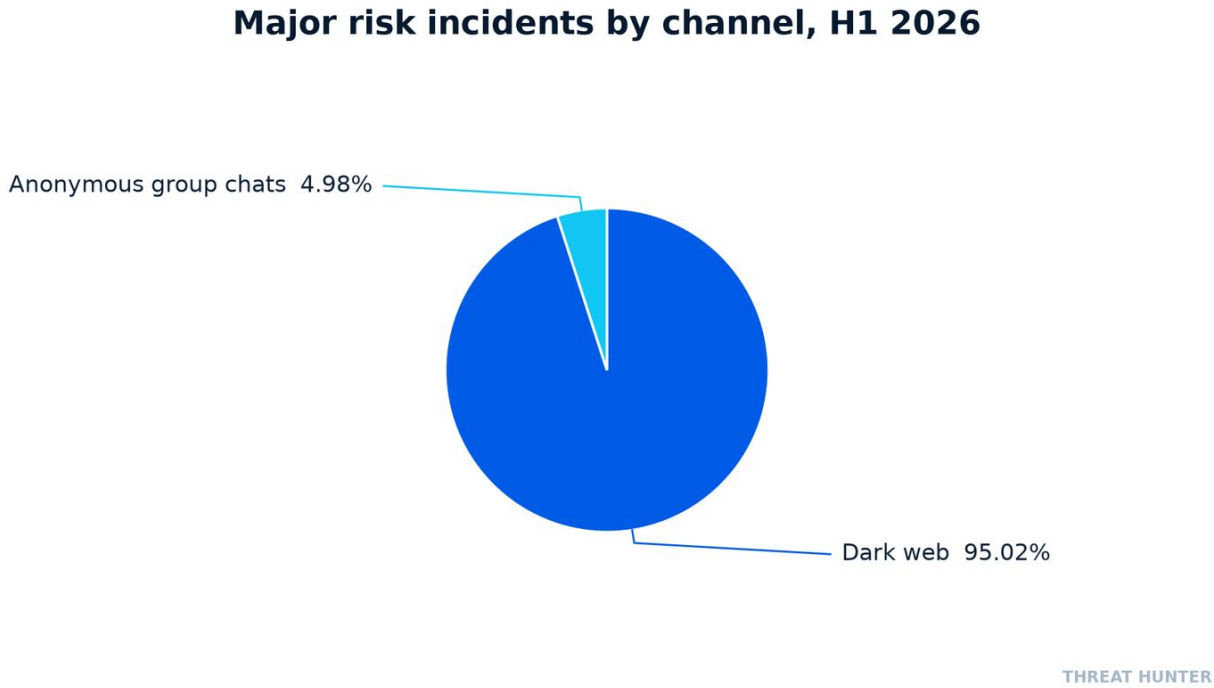
Compared with the overall number of incidents, the growth of major data leakage risk incidents is more obvious. A total of 542 major data leakage risk incidents were confirmed in the first half of 2026, an increase of 22.90% from 441 incidents in the second half of 2025. The major data leakage risk events mentioned in this report refer to events with large data magnitude, high field sensitivity, involving core business information, being publicly disclosed, or events that may cause greater impact on compliance, reputation, and public safety.

Among them, the proportion of darknet channels in major risk events increased from 76.64% to 95.02%, an increase of 18.38%. The dark web has become the main external channel for the public disclosure and dissemination of major data breach risks.



Major risk incidents by channel, H2 2025 vs H1 2026

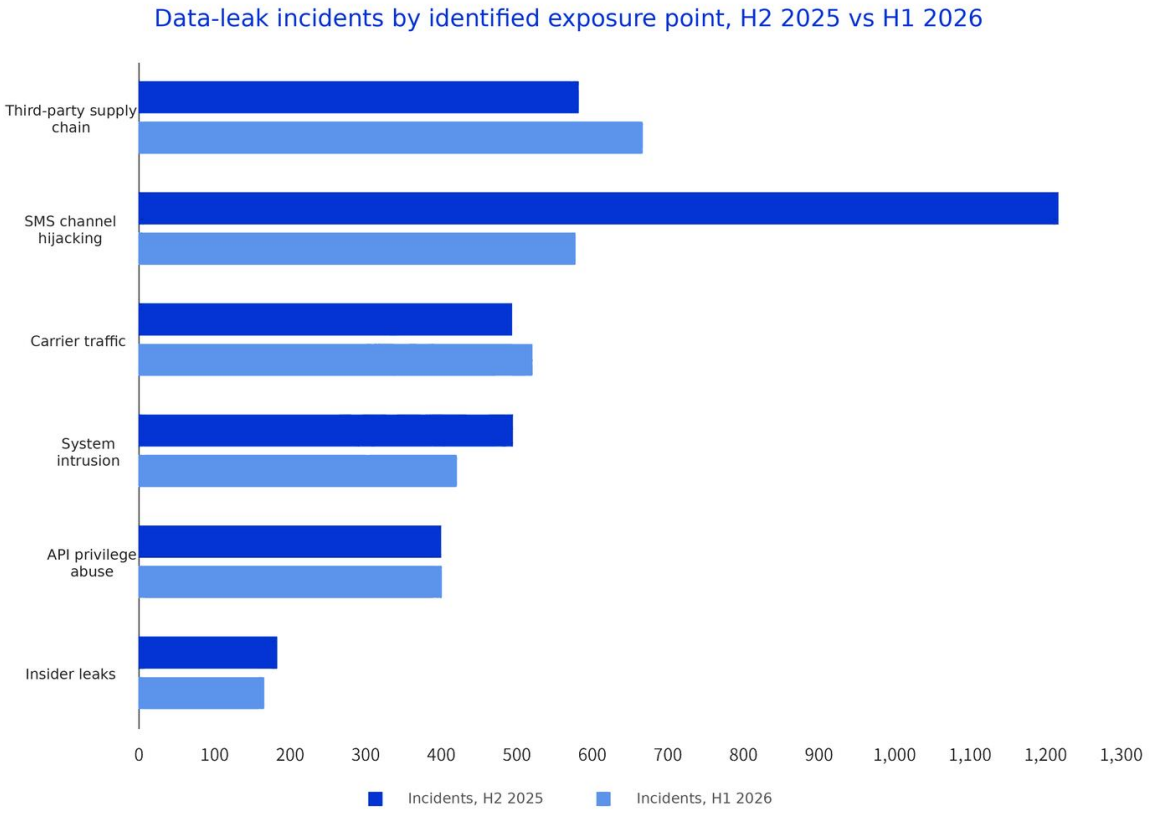
Source: Threat Hunter original report, page 8. Original figure with Chinese text replaced by English.



Major risk incidents by channel, H1 2026: the dark web accounts for 95.02%

Source: Threat Hunter original report, page 8. Redrawn in English from the original figure.

Judging from the identified risk sources, the leaked data involves third-party services, SMS channels, operator traffic, system penetration, API override and internal permissions, etc., reflecting that enterprise data exposure has extended from single system security issues to multiple types of external and internal nodes such as supply chains, communication links and permission management.



Data-leak incidents by identified exposure point, H2 2025 vs H1 2026

Source: Threat Hunter original report, page 9. Original figure with Chinese text replaced by English.

The risks faced by enterprises are no longer limited to "whether data is leaked", but also include what business data, accounts and access rights are possessed by external parties, whether the company name, data samples and attack statements are publicly disclosed and continue to spread, and whether this information continues to affect customers, partners and external reputational pressure.

1.3 Brand and channel abuse: The risk of counterfeiting is mainly distributed at the active search portals of multiple types of users.

In the first half of 2026, Threat Hunter detected a total of 45,321 phishing, counterfeiting and brand abuse risk incidents. Related risks appear in search results, counterfeit websites, social media, customer service hotlines, applications, download channels and other types of user active search portals.

Looking at the distribution of risk types, there were 20,726 SEO pollution records, accounting for 45.73%; counterfeit websites accounted for 29.56%. Search results and counterfeit pages are still

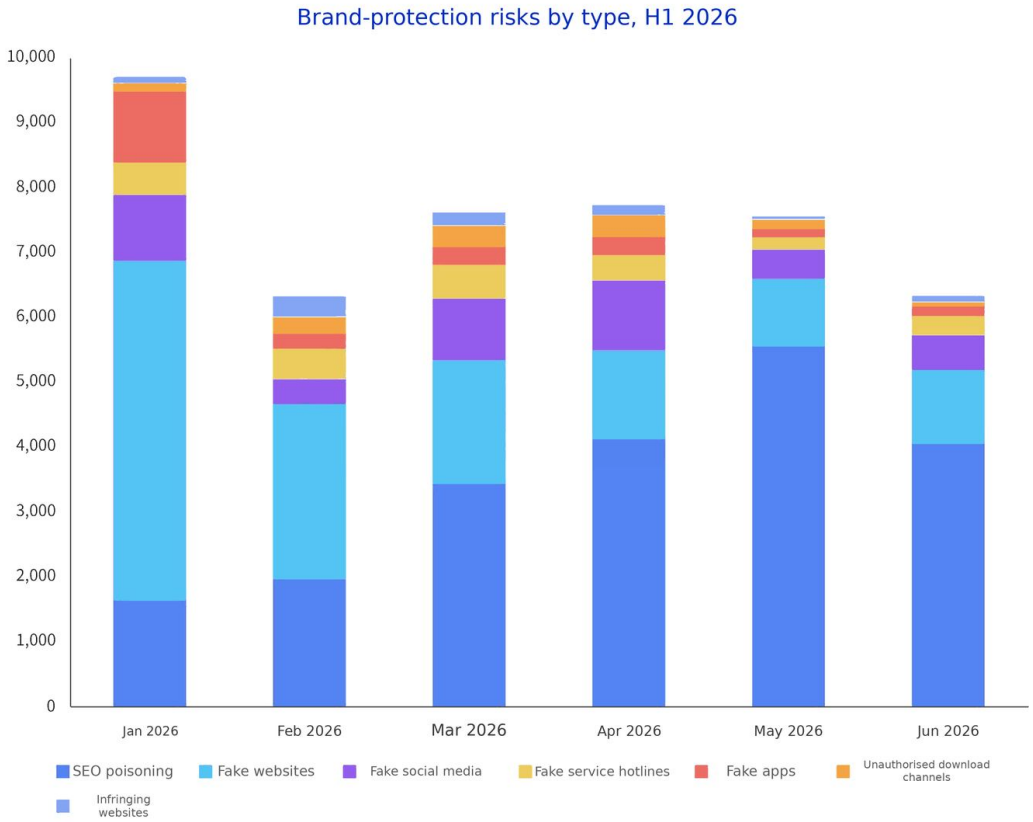
important places for brand abuse: the former may intercept users' needs when they are looking for customer service hotlines, account exception handling, refund claims, loan processing, or application downloads, while the latter may be responsible for information collection, malicious downloads, fake customer service contacts, or fund fraud.



Main types of brand-abuse risk, H1 2026: SEO poisoning 45.73%, fake websites 29.56%, other types 24.71%

Source: Threat Hunter original report, page 9. Original figure with Chinese text replaced by English.

In the first half of 2026, multiple entrances such as SEO pollution, counterfeit websites, counterfeit social media, counterfeit customer service numbers, counterfeit applications, unauthorized download channels and infringing websites continued to occur in parallel within half a year, and brand abuse was not concentrated on a single channel.



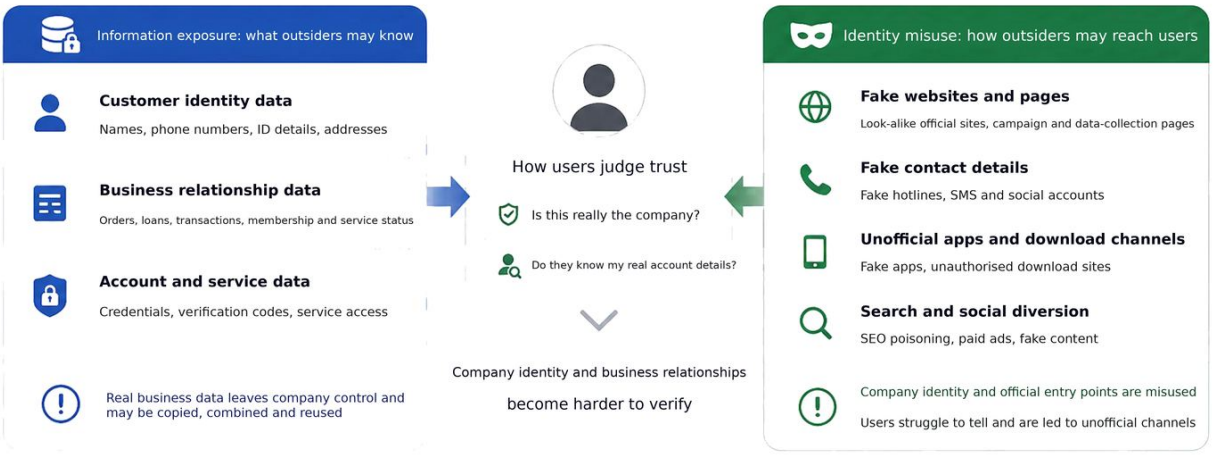
Brand-protection risks by type and month, H1 2026: no single channel dominates

Source: Threat Hunter original report, page 10. Original figure with Chinese text replaced by English.

Among them, infringing websites may impersonate the brand name, agent or partner identity, but do not directly show the intention of account theft or fund fraud; unauthorized download channels may distribute applications that are consistent with the official version, but have not been authorized by the brand. The harm paths of the two types of incidents are different from direct phishing, but they will weaken the company's control over brand identity, authorization relationships and download channels.

1.4 Information exposure and identity theft jointly erode brand trust

Users' trust in a company comes not only from identity indicators such as the company's name, website, account number, and customer service phone number, but also from whether the other party can accurately explain business information related to itself. Information exposure may provide external parties with real business details, while identity impersonation provides an entry point to contact users. Although the two types of risks appear in different forms, they will weaken users' ability to identify real corporate identities, official channels, and normal business relationships.



Information exposure and identity misuse together erode brand trust

Source: Threat Hunter original report, page 10. Original figure with Chinese text replaced by English.

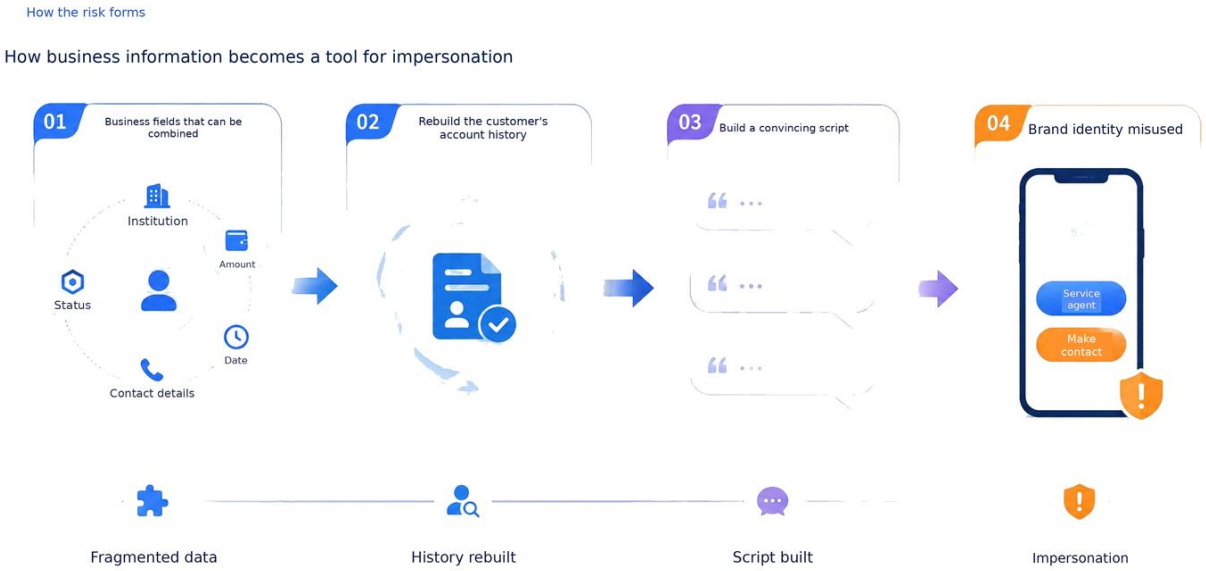
Brand protection needs to pay attention to both the information that external parties may possess and the entry points through which the corporate identity may be fraudulently used. Only by observing information exposure and identity fraud in parallel can we more completely identify the risks to user trust and official channels.

Chapter 2 How do brand external risks form?

Chapter 1 presents the scale and distribution of the two types of risks. This chapter further answers how these external signals enter the trusted relationship between enterprises and users. Risks are formed in different locations such as information, identity, entry and public communication, and do not follow a fixed attack chain.

2.1 How does business information become a condition for identity fraud?

When customers receive notifications related to customer service, collection, refund processing or account abnormality handling, an important basis for judging whether the other party is trustworthy is often whether the other party can tell details that are consistent with their business experience. Once fields such as institution name, amount, time, status, and contact information enter external channels, cybercriminal operators do not need to master the complete file, and may also use field combinations to restore a customer background that is sufficient to support impersonation.



How business information becomes a tool for impersonation

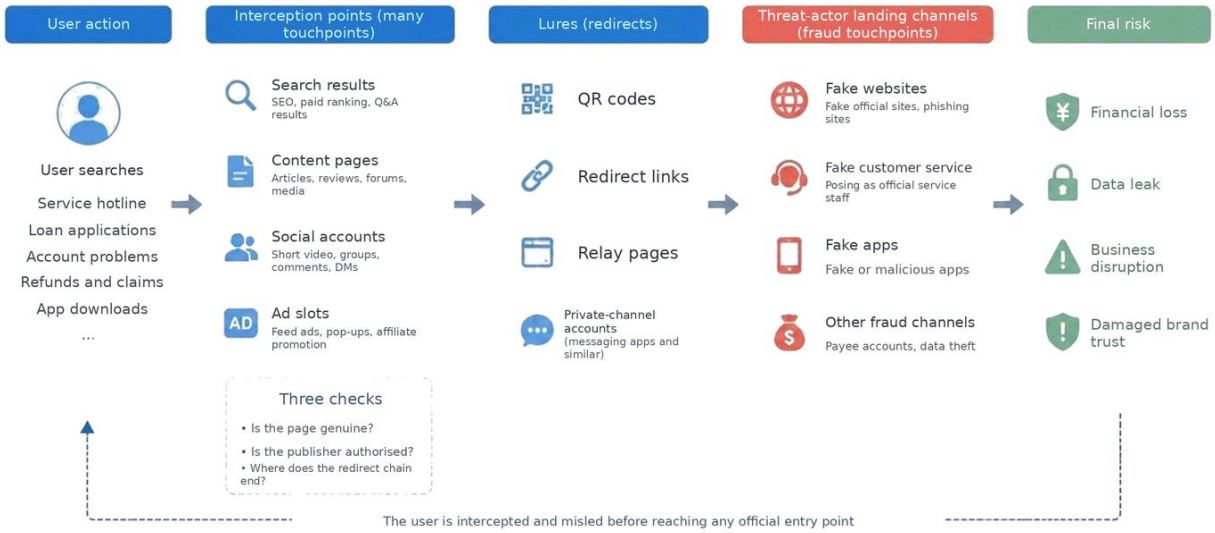
Source: Threat Hunter original report, page 12. Original figure with Chinese text replaced by English.

From the perspective of the risk formation process, the initial exposure may only be scattered fields; after screening, cross-reference, and classification by business stage, the fields can be transformed into object portraits and conversational clues. The real user-oriented risks occur in the next step: cybercriminal operations borrow corporate identities to contact users through phone calls, text messages, social accounts or fake pages, making real business details the basis for false trust.

Enterprises can block new data exposure and abuse paths through vulnerability repair, account disposal, and supplier rectification, but these measures cannot automatically clear out data that has been leaked, copied, and transferred. Even if the initial security incident has been dealt with, the relevant data may still be reused by cybercriminal operations. Therefore, customer relationship risks often do not disappear when security incidents end, but may continue to transform into subsequent impacts such as identity impersonation, precision fraud, customer complaints, and damage to brand trust.

2.2 Cybercriminal operations seize user access by counterfeiting information

When users actively search for information such as customer service phone numbers, loan processing, account exception handling, refund claims, or application downloads, they often have clear business needs. Cybercriminal operations place false information in search results, content pages, social accounts and advertising spaces, impersonating the company's official customer service, business channels or cooperative agencies, and intercept users before they enter the official website or contact official services. Subsequently, cybercriminal operations use QR codes, jump links, transfer pages or private domain accounts to guide users to counterfeit websites, fake customer service or other fraudulent channels.



How threat actors intercept users before they reach official channels

Source: Threat Hunter original report, page 13. Original figure with Chinese text replaced by English.

The interception entry itself may not be a fake page. Real-life content platforms, media pages or advertising spaces may also host unauthorized brand activities. Therefore, whether the page is authentic, whether the publishing subject is authorized, and where the jump link ends up are three issues that need to be judged separately. Chapter 4 will demonstrate this difference with a concrete sample.

2.3 Three types of easily confused channel risks

Counterfeit websites or applications, infringing websites and unauthorized download channels may all use company names, trademarks, product information or application materials. They are superficially similar, but the identification basis and main harm of the three types of risks are different. When making judgments, three aspects need to be observed: whether the relevant subject has forged the official identity of the company, whether the website or download channel has been authorized by the brand, and whether direct fraud such as account theft, malicious downloads, fake customer service, and induced payment has occurred in the current evidence.



Three channel risks that are easily confused: fake sites or apps, infringing sites and unauthorised download channels

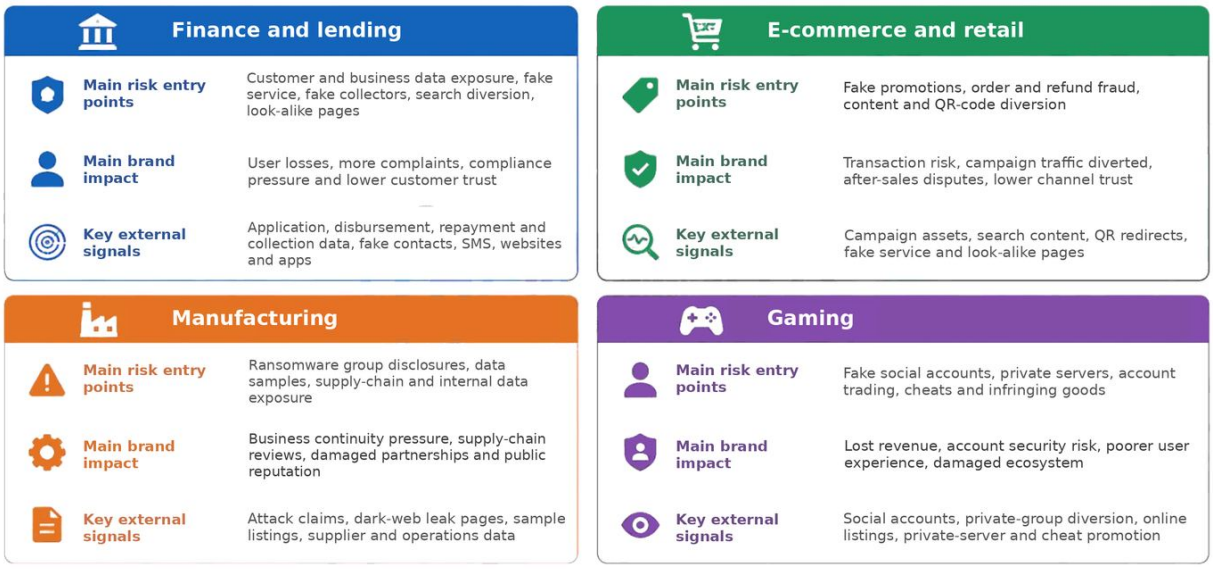
Source: Threat Hunter original report, page 13. Original figure with Chinese text replaced by English.

Transformations may occur between the three types of risks. For example, if the unauthorized download page subsequently replaces the installation package or adds fake customer service, the

nature of the risk will change; if an infringing website starts to collect credentials or induce payment, it is no longer just brand information that is being used without authorization. The point of classification is to accurately describe the current evidence, not to write off all unofficial entries as the same fraud.

Chapter 3 The external risk structures faced by different industries are significantly different

Different industries rely on different business relationships, user touch points and external platforms, and the main carriers, communication paths and impact results of brand external risks are also different.



External risk profiles differ by industry: finance and lending, e-commerce and retail, manufacturing, and gaming

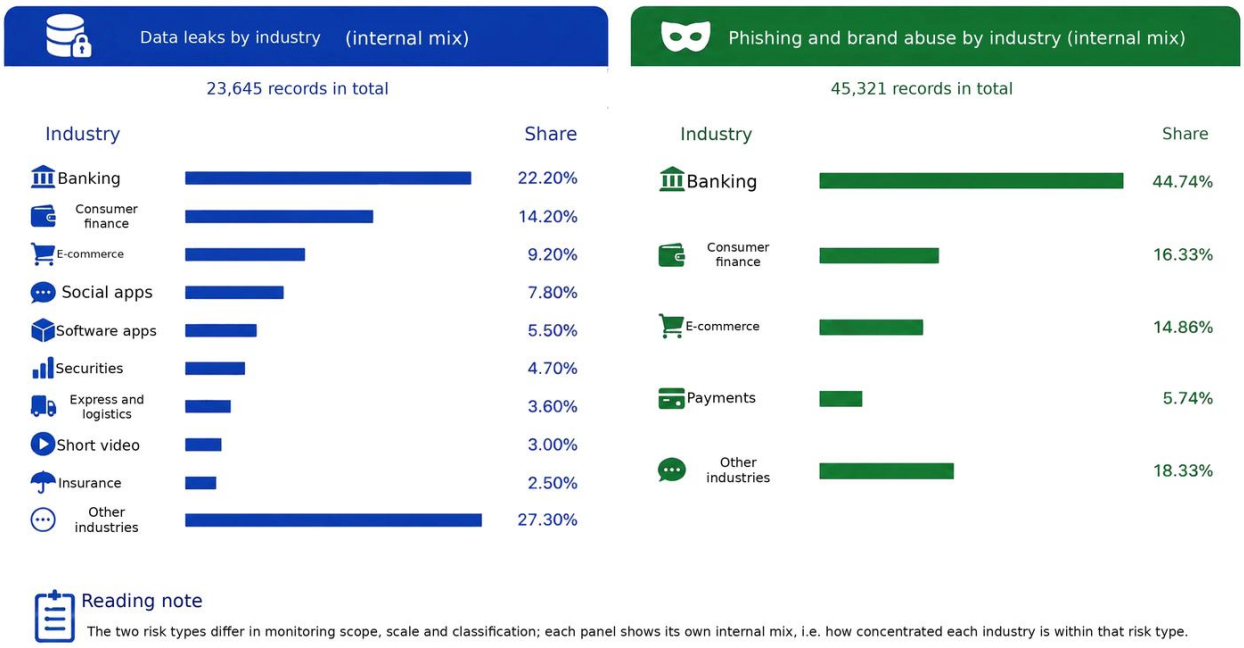
Source: Threat Hunter original report, page 15. Original figure with Chinese text replaced by English.

3.1 The financial industry is at a high level in both types of external risks

In the first half of 2026, financial-related industries will be in a high position in terms of data leakage risks and phishing and counterfeiting risks. Among the 23,645 data leakage risk events, banks recorded 5,251, accounting for 22.2%; consumer finance recorded 3,359, accounting for 14.2%. Among the 45,321 phishing and counterfeiting risk incidents, banking and consumer finance accounted for 44.74% and 16.33% respectively, and the payment industry accounted for 5.74%.

This distribution reflects that the financial industry not only faces the risk of customer and business information entering external channels, but also has long been affected by identity fraud problems such as counterfeit websites, fake customer service, search traffic, and unofficial applications. In addition to the financial industry, industries such as e-commerce, social tools, software

applications, securities, express delivery, short videos, and insurance also present external exposures of varying scales.



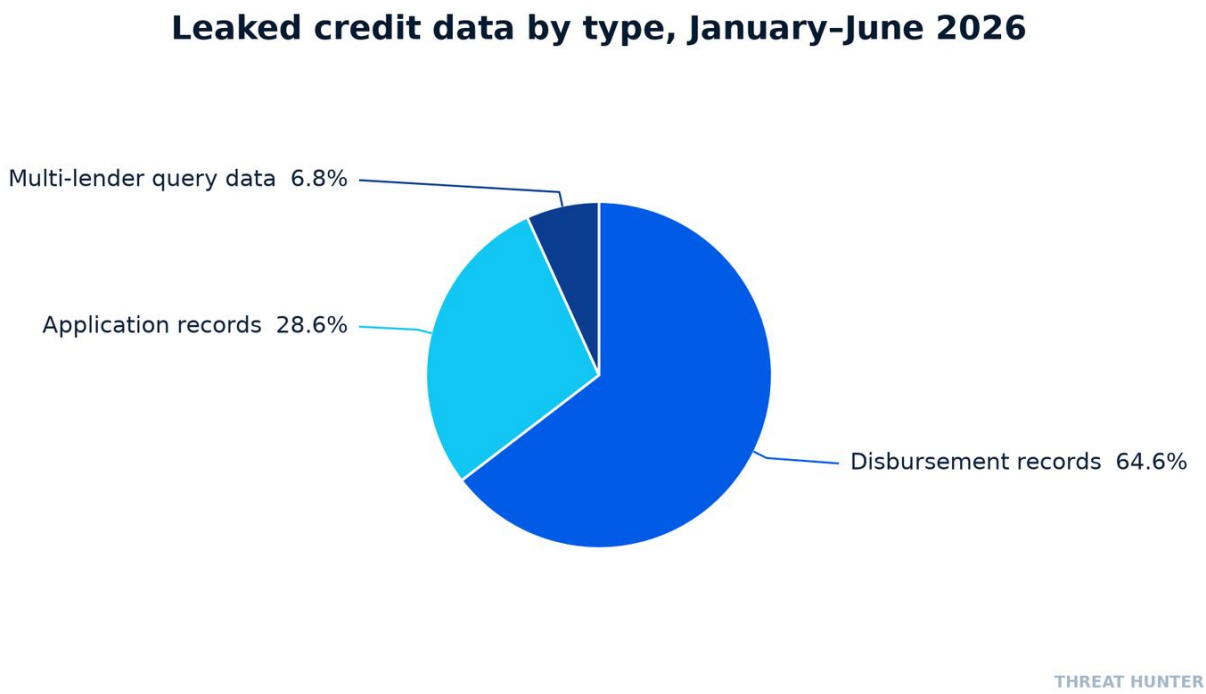
Industry mix within data-leak risk and within phishing and brand-abuse risk, H1 2026

Source: Threat Hunter original report, page 15. Original figure with Chinese text replaced by English.

3.1.1 The outflow of real business data in the financial industry intensifies the risk of identity fraud

Financial and lending business covers multiple aspects such as application, approval, lending, payment, repayment, collection and customer service. Relevant records usually include information such as customer identity, business status, transaction amount and contact information. Once this information enters external channels, it may not only expose personal information and business data, but may also be used to increase the confusion of false customer service, false collections, and other identity impersonation behaviors.

According to Threat Hunter analysis, among the loan data samples leaked in the first half of 2026, loan materials accounted for about 64.6%, application materials accounted for about 28.6%, and the rest mainly involved pre-loan query information such as long-term loans. Relevant records cover different business stages such as pre-loan application, loan approval and post-loan management, indicating that external circulation data is not limited to basic contact information, but may also reflect the true business relationship between customers and financial institutions.

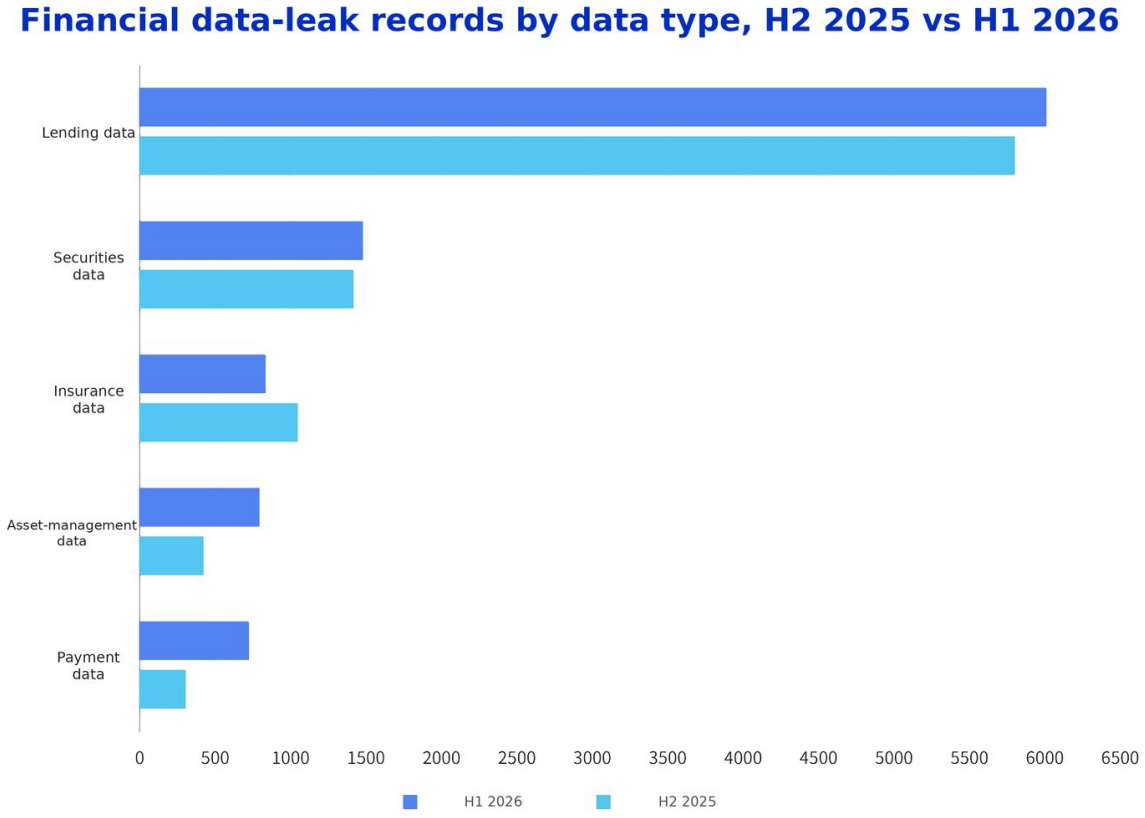


Leaked credit data by type, January–June 2026: disbursement records make up 64.6%

Source: Threat Hunter original report, page 16. Redrawn in English from the original figure.

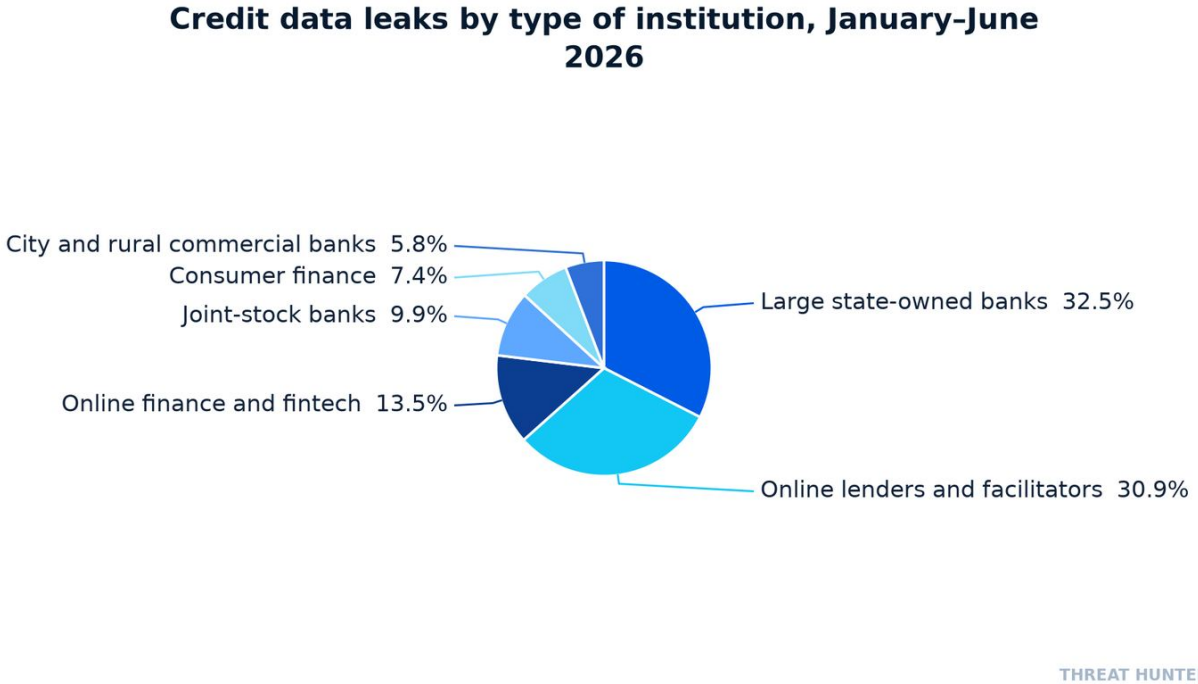
Threat Hunter monitoring found that compared with the second half of 2025, lending data risk records increased from 5,807 to 6,016 in the first half of 2026; asset management data increased from 428 to 799; payment data increased from 310 to 730, with the asset management and payment data increasing significantly.

Relevant lending data involves large state-owned banks, joint-stock banks, city and rural commercial banks, consumer finance companies, online small loans and loan assistance platforms, Internet finance and technology companies, etc., reflecting that risks are not concentrated in a single type of institution, but are distributed among different participants in the financial service chain.



Financial data-leak records by data type, H2 2025 vs H1 2026

Source: Threat Hunter original report, page 16. Original figure with Chinese text replaced by English.

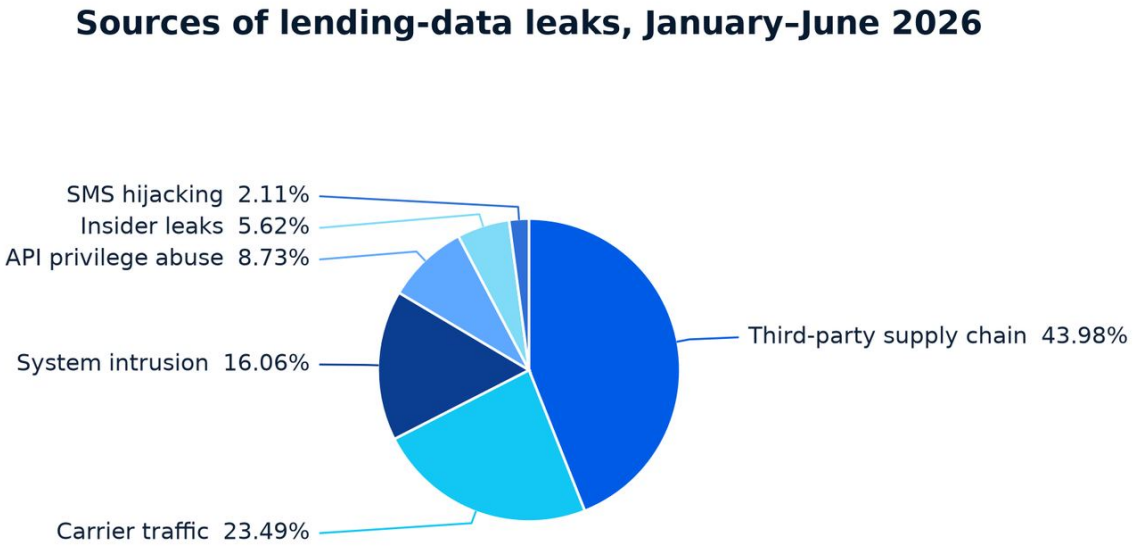


Credit data leaks by type of institution, January–June 2026

Source: Threat Hunter original report, page 16. Redrawn in English from the original figure.

Figure 3-3 Changes in financial data types and the structure of institutions involved in lending data

Judging from the identified exposure links, it mainly involves multiple nodes such as third-party services, operator traffic, system penetration, interface permissions, insiders, and SMS channels. Financial data may flow out of the institution's own system, or may appear in business connection links such as outsourcing services, communication links, interface calls, and cooperative institutions.



Sources of lending-data leaks, January–June 2026: the third-party supply chain accounts for 43.98%

Source: Threat Hunter original report, page 17. Redrawn in English from the original figure.

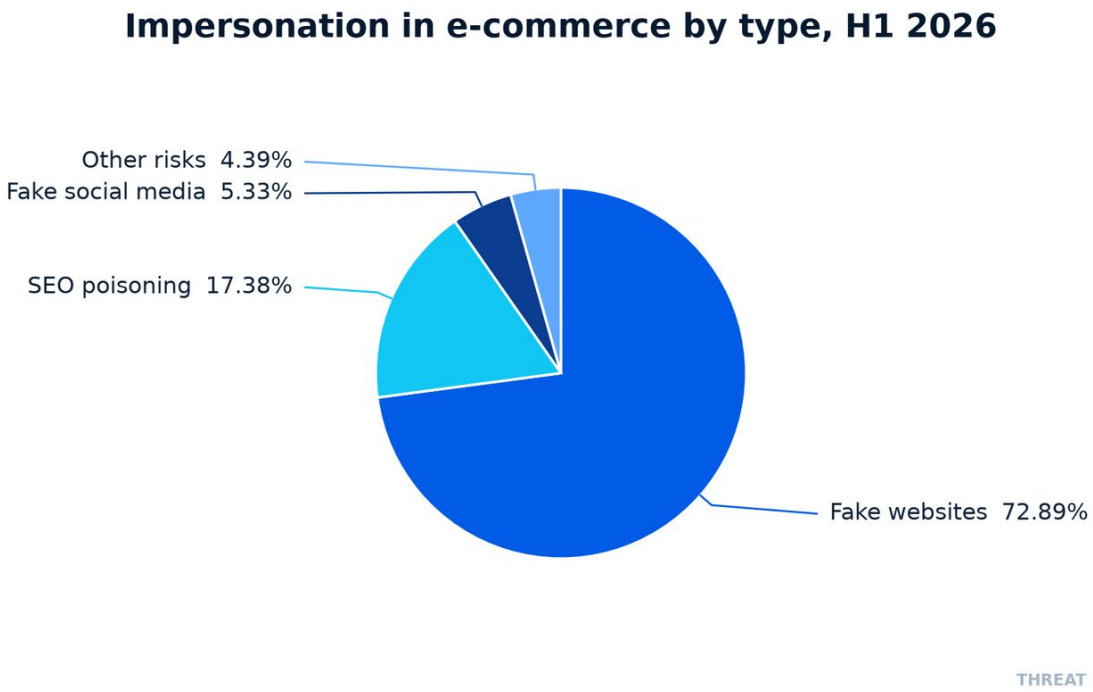
The brand risk of financial institutions is therefore not only reflected in the fraudulent use of names, websites or customer service numbers, but is also closely related to whether customer business information is out of control. When external parties have access to loan status, transaction amount, repayment time or service records, content pretending to be customer service, collection or business personnel is more likely to gain user trust and may further lead to information leakage, financial losses, customer complaints and brand reputation risks.

3.2 E-commerce industry: risk of abuse of consumer-facing channels

In the first half of 2026, a total of 6,736 phishing and counterfeiting risk incidents were discovered in the e-commerce industry, which is the scenario with the highest concentration of risks outside the financial-services sector.

In terms of risk types, counterfeit websites are the most important risk type in the e-commerce industry, with a total of 4,910 cases, accounting for 72.89%; SEO pollution cases, 1,171 cases, accounting for 17.38%; counterfeit social media cases, 359 cases, accounting for 5.33%. Among them, the total proportion of counterfeit websites and SEO pollution reached 90.27%, indicating

that the risk of phishing and counterfeiting in the e-commerce industry is mainly concentrated in the two links of "search traffic" and "counterfeit page acceptance".



Impersonation in e-commerce by type, H1 2026: fake websites account for 72.89%

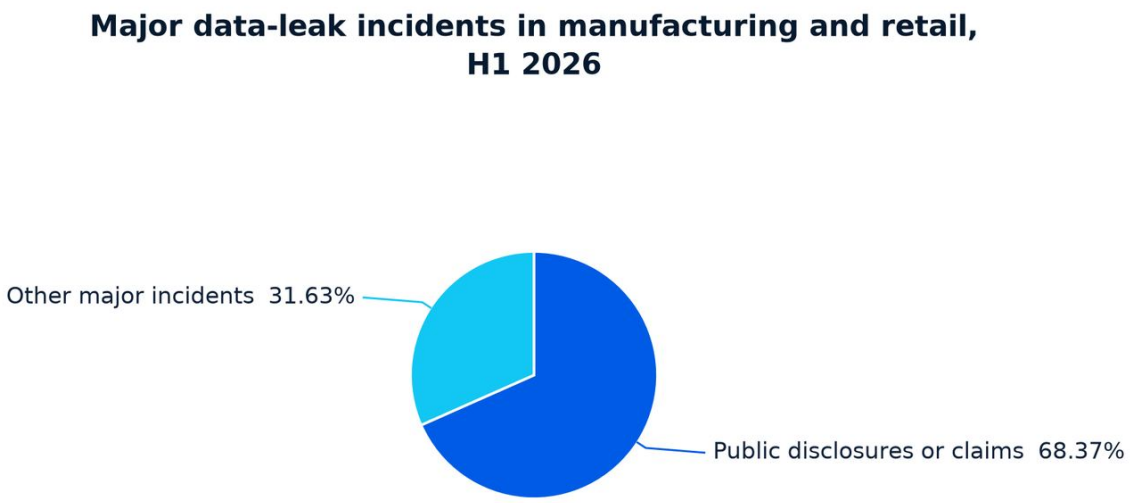
Source: Threat Hunter original report, page 18. Redrawn in English from the original figure.

Relevant risks usually revolve around high-frequency scenarios such as promotional activities, order anomalies, refund claims, logistics notifications, and platform customer service. Attackers take advantage of users' concerns about price concessions, order timeliness and after-sales processing, intercept demands through search results, content advertisements or QR codes, and then direct users to fake activity pages, login pages, payment pages or private domain customer service to implement information collection, malicious downloads or fund fraud.

3.3 Manufacturing and retail industries: major data breach and public disclosure risks

In the first half of 2026, major data leakage risk events in the manufacturing industry increased by 82.14% compared with the second half of 2025; the retail industry increased by 59.26%. The growth rate of the manufacturing industry is even more prominent, and the potential impact of major risk events on corporate production operations, cooperative relationships, and public reputation has further increased.

Among the major risk events discovered in the manufacturing and retail industries, 68.3% appeared on the public release page of ransomware organizations or related sites. The public display of company names, attack statements, and data samples has become an important way for relevant risks to enter the eyes of customers, suppliers, partners, and the public.



Major data-leak incidents in manufacturing and retail, H1 2026: public disclosures or claims make up 68.37%

Source: Threat Hunter original report, page 19. Redrawn in English from the original figure.

Judging from the public disclosure incidents related to the manufacturing and retail industries in China in the first half of 2026, The Gentlemen recorded 23 incidents and Qilin recorded 17 incidents. The number of incidents was significantly higher than other entities; Akira and Inc Ransom each recorded 10 incidents, and LockBit 5.0 and DragonForce each recorded 9 incidents.

On the whole, related incidents show that the leading subjects are more prominent, and the participating subjects are relatively dispersed. The manufacturing and retail industries continue to become important targets for extortion organizations to publicly list and issue attack statements.



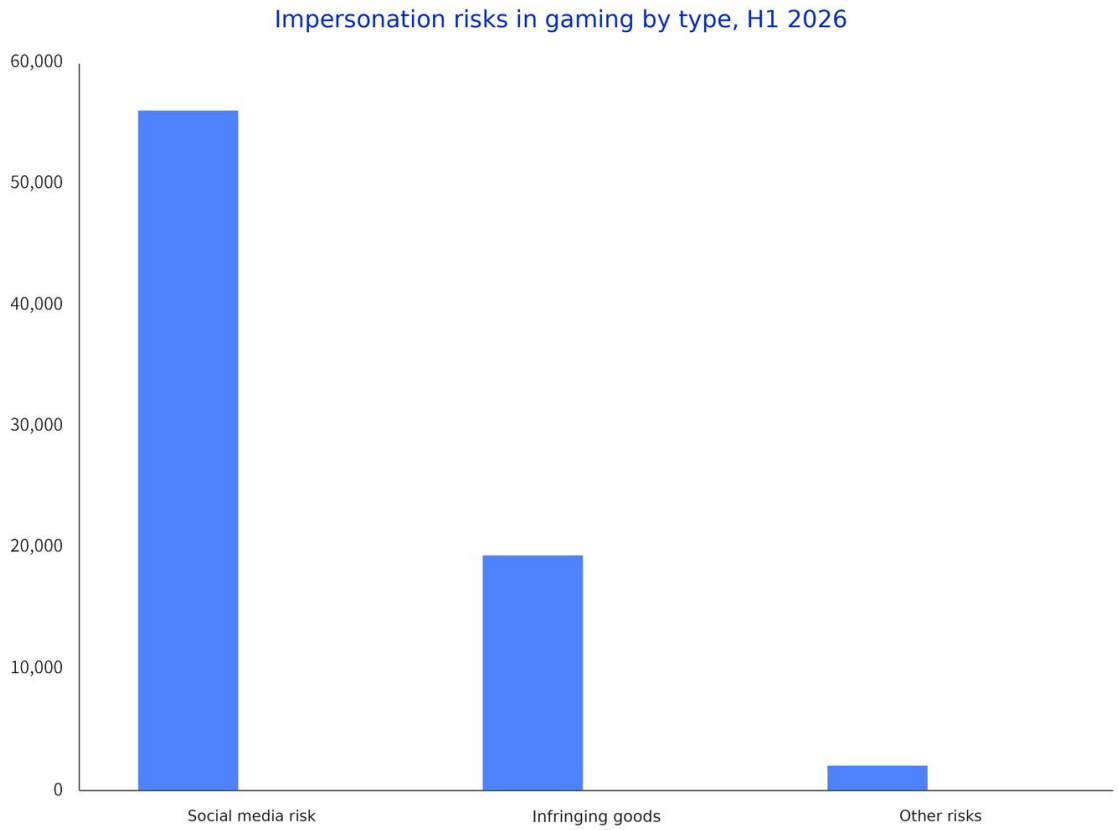
Top 10 groups by public disclosures of manufacturing and retail victims in China, H1 2026

Source: Threat Hunter original report, page 20. Original figure with Chinese text replaced by English.

In the first half of 2026, more than two-thirds of major risk events in the manufacturing and retail industries were publicly disseminated through relevant organizations or sites. This means that the impact of related risks is no longer limited to technical disposal within the enterprise. Manufacturing incidents may further affect production arrangements, supplier collaboration and business continuity; retail incidents may directly trigger consumers' concerns about transaction security, personal information protection and service reliability. As company names, attack claims and data samples are publicly displayed, customer trust, partner vetting, supply chain relationships and public reputation may all have ongoing impacts.

3.4 Game Industry: Social Communication and Product Infringement Form an Independent Ecosystem

In the first half of 2026, a total of 77,816 related risks were recorded, including 56,071 cases of social media counterfeiting, 19,350 cases of product infringement, and 2,395 cases of other risks. This total should not be directly added to or compared horizontally with the aforementioned data.



Impersonation risks in gaming by type, H1 2026: social media risk leads, followed by infringing goods

Source: Threat Hunter original report, page 20. Original figure with Chinese text replaced by English.

Counterfeit social content usually attracts players with benefits, redemption codes, scarce resources or version advantages, and then guides them into private channels. Product infringement mainly involves e-commerce products such as private servers, BT servers, modified versions, finished accounts, plug-ins, auxiliaries and scripts, which directly causes revenue diversion and may affect account security, game fairness and user experience.

Among the 19,350 special records of product infringement monitored by Threat Hunter, there were 7,933 cases of private servers, BT servers and modified versions, 6,305 cases of account transactions, and 1,198 cases of plug-ins, auxiliaries and scripts. Game counterfeiting incidents mainly focus on private servers, accounts, plug-ins and other products on e-commerce platforms, which are different risk forms from the infringing websites mentioned above.



Infringing gaming goods by subtype: 19,350 records, led by private servers and modded versions

Source: Threat Hunter original report, page 21. Redrawn in English from the original figure.

Figure 3-11 Samples of counterfeit social media and product infringement in the game industry

The main objects of observation for game risks are social accounts and e-commerce products. The difficulties lie in fragmented platforms, multiple content variations, rapid account reconstruction, and repeated listing of products. Its identification and disposal path is obviously different from the risk path in the financial industry around search portals, customer service and high-imitation pages.

Chapter 4 Typical Cases of Brand External Risks

External brand risk rarely stops at a single page or data record. Content publishing, jump control, data packaging and identity impersonation are often scattered in different links. Continuing verification along the sample will help restore the content that the user finally came into contact with and the link where the brand was used fraudulently. The following are 2 typical cases detected by Threat Hunter.

4.1 Credibility is “hijacked”: Cybercriminal operations rely on authoritative integrated media channels to attract traffic

In the first half of 2026, Threat Hunter discovered a new method of using the credibility of the media to carry out counterfeit traffic. Cybercriminal operations no longer rely solely on self-built websites or low-weight social accounts for communication, but contact financial media, industry media and local information public accounts in the name of "advertising", publish promotional articles that impersonate a leading e-commerce brand through formal content channels, and use the authoritative attributes of media accounts to reduce user alertness.

Relevant content usually uses notification-style titles such as "Arrival soon! Citizens please prepare!" and replaces the city name according to the delivery area. During the same period, multiple pieces of content with highly similar title structures, campaign materials, and traffic drainage methods were detected. The release times and release channels were scattered, showing the characteristics of template production, cross-regional delivery, and batch copying.



Search results for look-alike articles posted on a converged-media platform under titles such as "Arriving soon, get ready!"

Source: Threat Hunter original report, page 23. Original image retained.

The text of a typical article only contains a long picture of the activity and a QR code. It uses continuous sign-in to receive free daily necessities, small household appliances and smart digital products as a bait to guide users to scan the code, download and install the application and complete the registration. After verification by the brand owner, the relevant activities were not authorized, and the brand authorization documents and official authorization seal submitted by the publisher were forged.

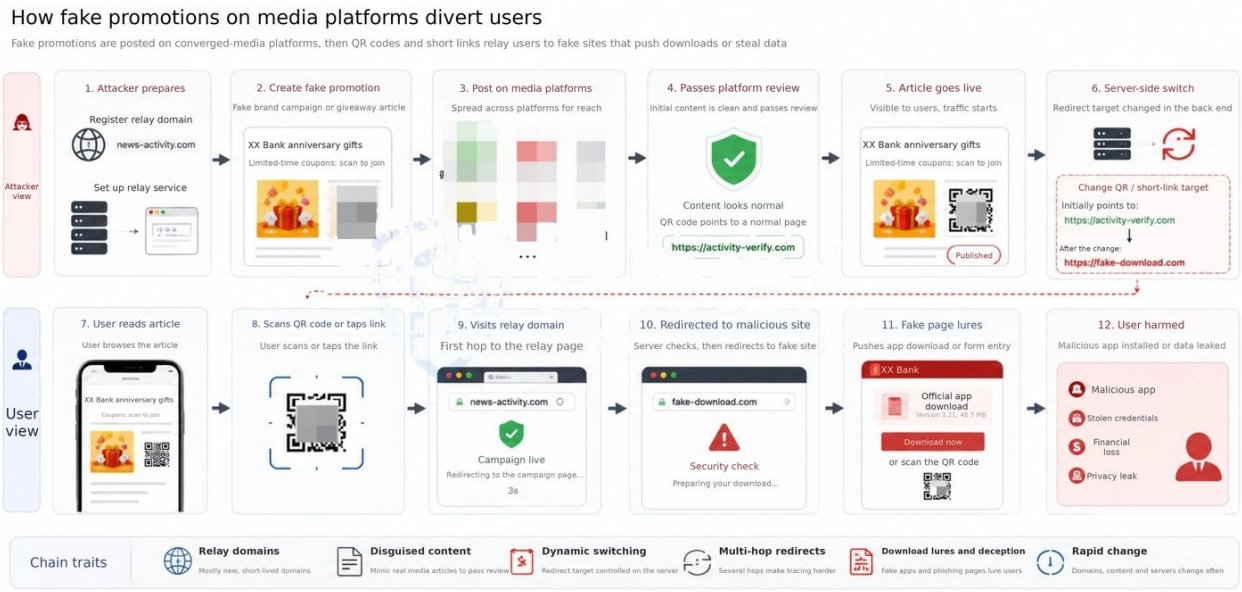


A fake "daily check-in gifts" promotion that asks users to scan a QR code and install an app

Source: Threat Hunter original report, page 24. Original image retained.

4.1.1 Malicious links

Compared with traditional counterfeit websites, the risk of this method is not only in the final landing page, but also in the attacker's use of formal communication channels to complete "trust transfer." Users tend to equate "the release channel is credible" with "the activity is authentic and credible"; during the ad review process, media operators tend to pay more attention to qualification documents, promotional content and the results of the first scan, making it difficult to continuously observe the access target behind the QR code. Since the QR code always points to the same transit entrance, there is no need to modify the article content or QR code pattern when changing links on the server side. The page seen during the review may be different from the page that the user subsequently visits, making it difficult to detect abnormalities in a timely manner through regular review and single QR code scanning.



How fake promotions on converged-media platforms divert users: pass review with clean content, then switch the redirect on the server

Source: Threat Hunter original report, page 24. Original figure with Chinese text replaced by English.

This model reflects three obvious changes:

- Make communication channels credible. Cybercriminal operations have shifted from low-weighted accounts to integrated media and local information channels, using media influence to complete the first endorsement.
- Inducing content into pictures. Brand names, promotional words and QR codes are concentrated in the long activity image, reducing risk characteristics that can be identified by text rules.
- Audit avoidance becomes dynamic. The QR code entrance remains unchanged, the back-end access target can be adjusted in stages, and a single verification cannot reflect subsequent risks.

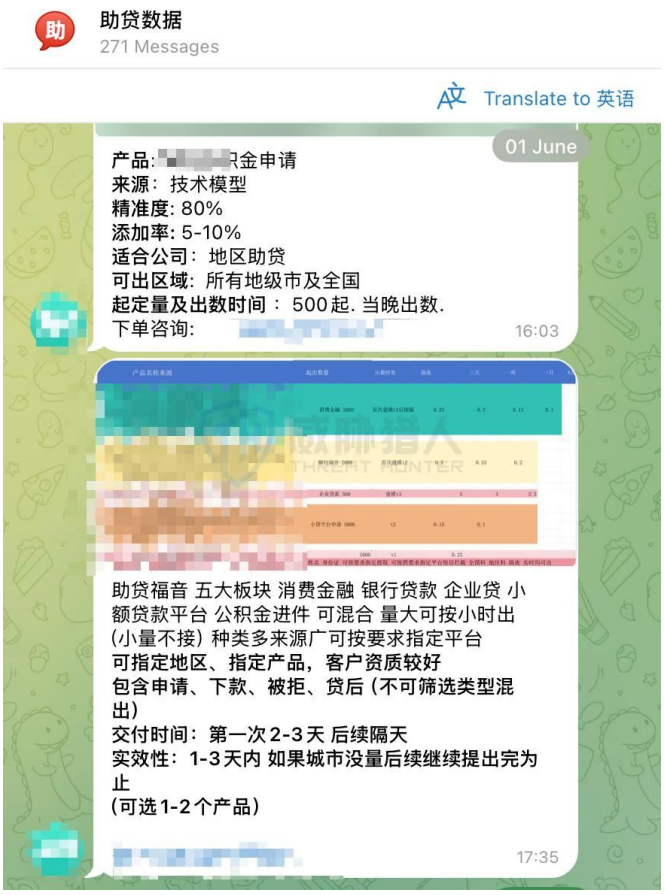
This type of attack will affect users, media and counterfeited brands at the same time: users may reduce their awareness of verification because they trust publishing channels; media accounts may become risky traffic portals without knowing it; counterfeited brands need to bear the inquiries, complaints and loss of trust caused by unofficial activities. The harm has extended from the imitation of a single brand to the dual erosion of media credibility and brand channel order.

4.2 Typical ways in which real business information and counterfeit channels jointly create the illusion of “official collection”

Fake collection is a typical case where information exposure and identity impersonation are combined in the same business scenario. Threat Hunter monitoring found that some fraud gangs will purchase loan user data from the illegal data trading market. After obtaining the user's application, loan or overdue information, they will then contact the user through false collection text messages, customer service calls and high-imitation repayment pages. What users are faced with is not a piece of unfamiliar information without any basis, but a set of "official collection" illusions that contain both real business details and corporate brand identity.

4.2.1 Real business information first fills in the details required for “collection”

Lending data circulating through underground channels is usually classified by business status such as application, loan, and overdue. In addition to basic information such as name and phone number, relevant samples may also include loan platforms, application or loan time, loan amount, overdue status and bank card information. Compared with ordinary contact information lists, these fields can restore the true business relationship between the user and a certain financial institution, and also provide a more confusing basis for subsequent communication by pretending to be customer service or collection personnel.



A threat actor advertises leaked loan-facilitation data with accuracy rates, delivery times and prices

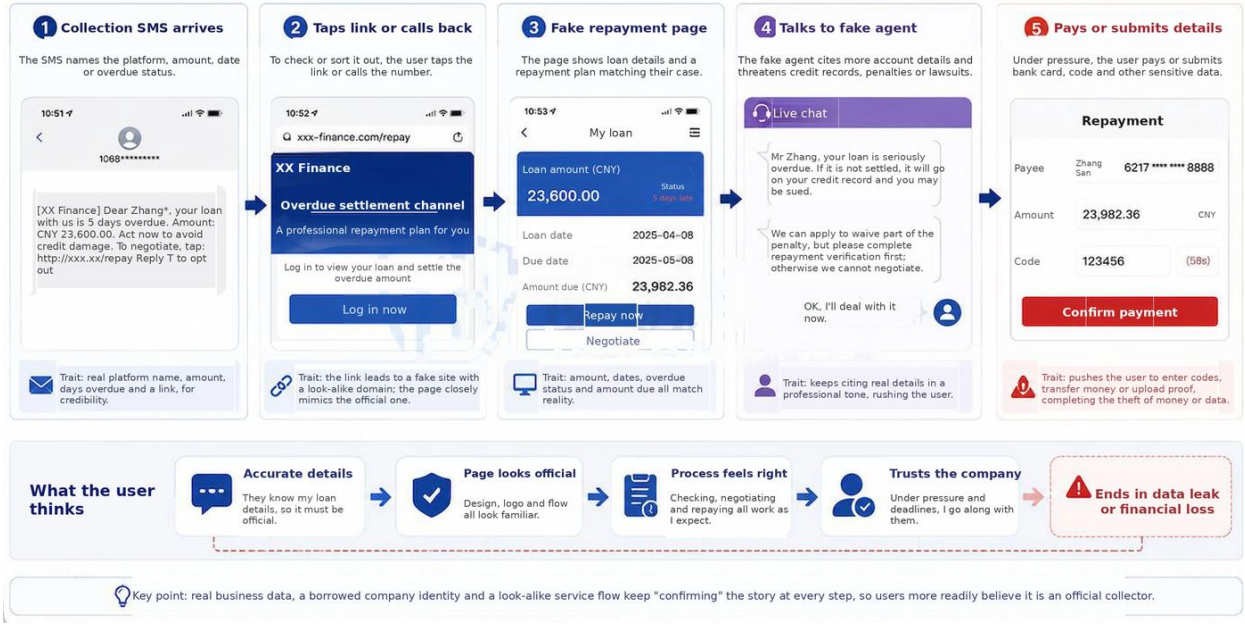
Source: Threat Hunter original report, page 26. Original image retained.

4.2.2 False text messages and high imitation pages jointly strengthen the illusion of “official collection”

After obtaining relevant data, the fraud gang initiates contact with users through collection text messages, virtual numbers or social tools. The content of the text message may directly show the loan platform, loan amount, application time or overdue status, with so-called "query contract" and "negotiate repayment" links attached. The page that the user enters after clicking further uses the company name, logo, business language and repayment process, so that the real business information in the previous link can be "verified" visually and through channels.

4.2.3 What users see is a continuous “official collection” link

In this process, the real business information answers the user's question "Why does the other party know my situation?", while the company name, text messages, customer service and repayment pages answer the question "Why does the other party look official?" The two types of information reinforce each other in successive touch points, making it more difficult for users to identify real service entities and unofficial channels.

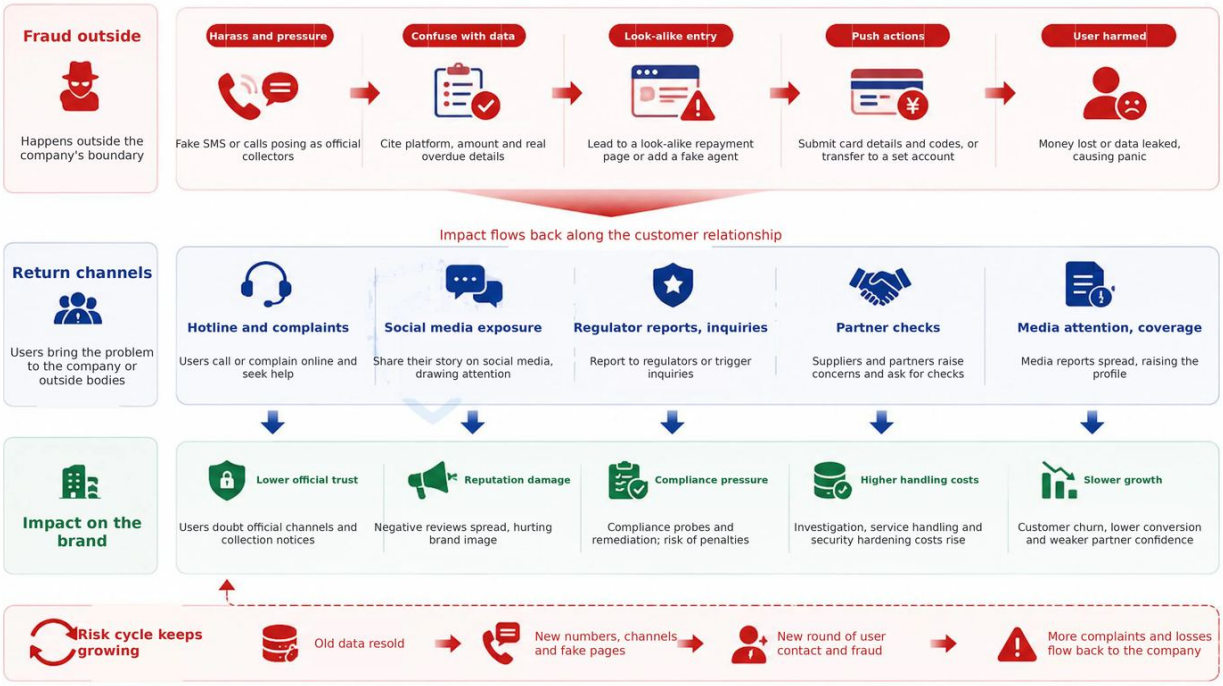


What the user sees: a fake "official collection" that confirms itself at every step

Source: Threat Hunter original report, page 27. Original figure with Chinese text replaced by English.

4.2.4 Fraud occurs outside the boundaries of the enterprise, but the impact will return to the brand

Although the fake reminder behavior occurs outside the control of the company, users are exposed to the company name, real loan information and highly similar service pages. Once harassment, information leakage or financial loss occurs, users will often associate the relevant experience with the fraudulent financial brand, further forming complaints, doubts and distrust of official collection channels.



The fraud happens outside the company, but the impact flows back to the brand

Source: Threat Hunter original report, page 27. Original figure with Chinese text replaced by English.

Even if the initial data exposure portal has been repaired, historical data entering underground channels may still be copied, resold, and reused through new SMS numbers, customer service accounts, and fake pages. Therefore, related risks will not automatically end with a single vulnerability fix or page delisting, but may continue to return to the user side through new contact vectors.

This case illustrates that brand protection not only requires identifying pages, accounts, and contact information that are fraudulently using corporate names, but also requires attention to whether real business information that is sufficient to support identity fraud has entered external channels. Once the circulation of customer relationship data is combined with the fraudulent use of corporate identity, the impact of external fraud may continue to flow back to the brand along the paths of complaints, risk signal, and supervision.

Therefore, enterprises need to cut off the complete link of "data leakage □ identity theft □ user victimization □ influence backflow" before the risk flows back and spreads to the brand level, which is also the core goal of brand protection.

Conclusion

This report is compiled by the Threat Hunter anti-fraud intelligence research team based on long-term monitoring data, real risk samples and industry governance practices. External risks to corporate brands will not stop at a single counterfeit page or a data leak. Risks such as data exposure, identity fraud, channel interception and public dissemination will continue to evolve and continue to affect the trust relationship between enterprises and users. Threat Hunter will continue to collaborate with enterprises in various industries to jointly improve the ability to discover, analyze and deal with external brand risks, and protect corporate brand security and user rights.

It is hoped that this report can help brand protection, security, fraud controls and business practitioners more accurately understand the changes in external risks of corporate brands, identify the main risk structures and formation paths in different industries, and provide a reference for enterprises to formulate more targeted brand protection and external risk governance strategies.