THE THREAT LANDSCAPE OF THE TOP LUXURY BRANDS IN FRANCE

KELA

The Threat Landscape of the Top Luxury Brands in France

Laura Weinberg, Threat Intelligence Analyst

Introduction

The luxury sector is considered particularly dynamic in France due its traditions, manufacturing expertise and craftsmanship. With five French companies in the top 10 luxury brands for 2021,[1] France is a world leader in the sector, with around 150 billion EUR in revenue for 2021.[2]

Luxury companies' clientele holds private data from typically wealthier individuals and potentially public figures, which makes these businesses even more attractive targets. Luxury brands provide a more tailored service to their clients, and as a result, the data they collect may be more detailed than that of other retailers.

For example, the Korean branch of the French luxury company Chanel was hit by a cyberattack in August 2021. Following the attack, a client database that included names, birthdays, phone numbers, and product purchase lists was leaked. Customers demanded to be compensated and said they expected better security and higher services from such a company.[3]

Employees' data may also be compromised and could provide a foothold into a company's internal system, giving attackers access to valuable internal data that they may want to exfiltrate and sell or use to extort the company.

Considering what is at stake, KELA decided to research cyber threats the French luxury sector faces, including sellers of counterfeits and refund methods targeting French luxury brands. In addition, KELA researched the sector's threat landscape by focusing on the top 10 companies. Mentions of France's top luxury brands were collected to evaluate the sector's exposure to cyber threats concerning leaked

[1] Global Powers of Luxury Goods 2021
[2] French (CAC) Luxury Industry Analysis
[3] Chanel Apologizes for Data Breach

credentials and compromised accounts[4] based on the cybercrime underground sources that KELA monitors. The analysis focuses on 10 of France's top luxury brands and groups, including global and local domains. Finally, KELA took a look at Initial Access Brokers and ransomware attackers targeting the sector.

Below are KELA's key findings in its research on the French luxury sector cybercrime threat landscape:

- Threat actors use cybercrime underground marketplaces and social media platforms to sell counterfeit luxury goods. They openly advertise their products as counterfeits and indicate the level of quality of the forgeries that are sold for a fraction of the genuine item's market price.
- Online fraudsters abuse luxury brands by conducting refund scams which enables them to order expensive luxury products and then get a refund whilst keeping the items. Threat actors often share or sell their methods in underground forums.
- Sensitive data held by luxury companies is especially valuable to cybercriminals and data from French companies was found to be highly in demand in underground forums, including threat actors looking for data from high-end businesses, or selling clients' databases from luxury shops.
- KELA's research into the exposure of 10 French luxury companies highlighted that most leaked credentials appeared in breaches of companies that aren't part of the luxury sector, such as the Apollo breach and the People Data Labs breach. KELA's review also uncovered critical access to internal corporate services, including an internal password reset platform or third-party vendor portals, which were compromised and offered for sale in automated markets.
- Network accesses to French companies were found for sale on underground forums, and one targeting an iconic French luxury fashion brand was detected.
- During 2020-2022, a period during which ransomware groups' activity drastically increased, at least 24 French companies from the retail sector were targeted by the ransomware groups.

[4] See the terms' explanation in the relevant chapters.

Counterfeits

The counterfeit market has flourished online, and fraudsters are using the anonymity offered by online platforms to sell fake products. In 2021, French customs seized around 9 million counterfeited products, a 62% increase over the previous year.[5] That same year, the cost of counterfeits was estimated to surpass 6 billion EUR in France,[6] according to Unifab (Union des Fabricants), "a recognized public-interest organization" that "promotes international protection of intellectual property fighting against counterfeiting."

Cybercrime forums, marketplaces and social media platforms are channels favored by cybercriminals to conduct illicit trades. The luxury industry is particularly affected by this because the high cost of items may provide large benefit margins for threat actors and the demand for such products tends to be high. KELA has reviewed luxury counterfeits from several French brands offered for sale by cybercriminals on cybercrime underground sources, as well as on social media.

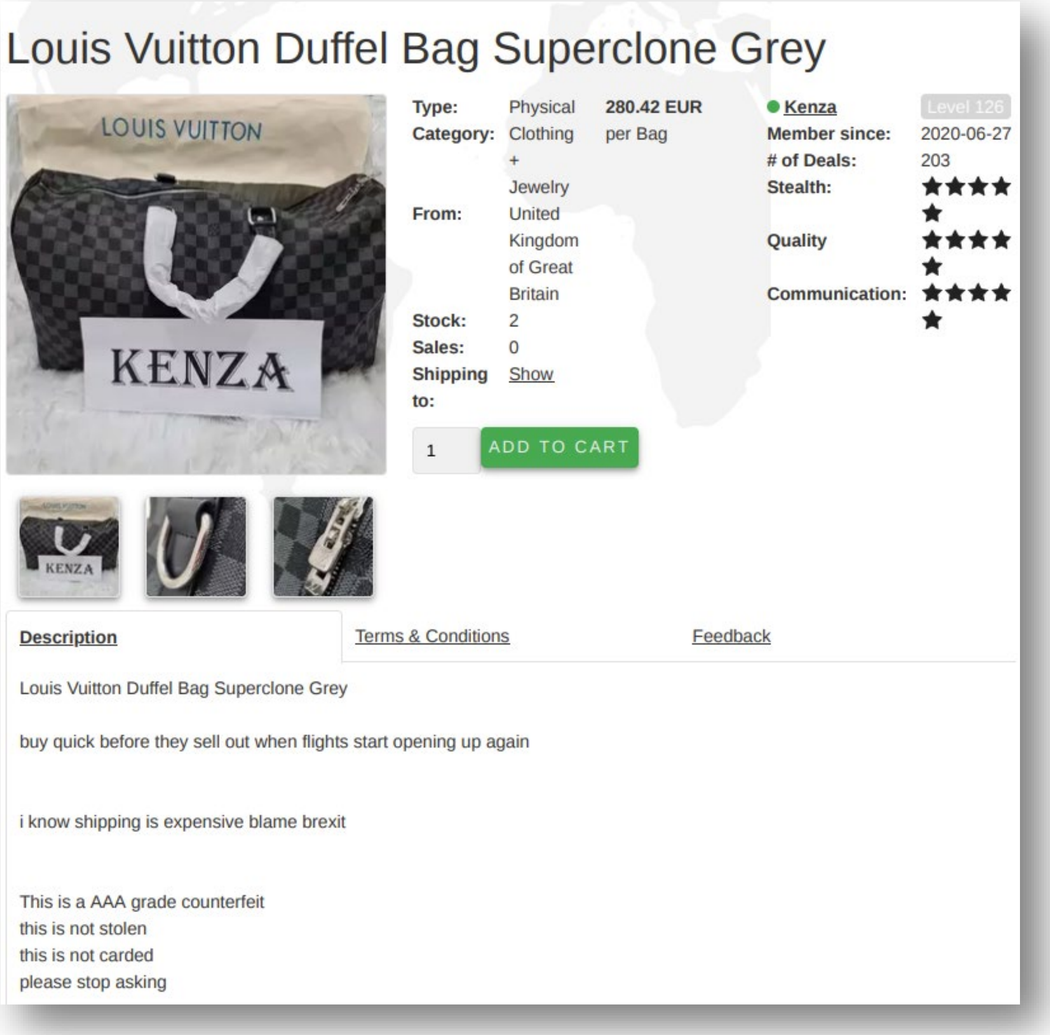
Cybercrime Underground Sources

Due to their illegal nature, counterfeit goods are often found for sale on platforms that offer a higher level of anonymity. Cybercrime forums and marketplaces don't tend to focus only on these types of goods but often offer a large range of products and services. Cybercrime underground marketplaces are used to resell all sorts of illegal goods, including drugs, weapons and counterfeit items. Users can buy or sell relatively anonymously and can rate the quality of the items purchased, as well as the seller's service and communication. Transactions are often, if not always, done using cryptocurrencies.

For example, a fraudster registered under the username "Kenza" on the now-defunct Versus Project Market posted an advertisement for "Louis Vuitton Duffel Bag Superclone Gray" and described the item as "AAA grade counterfeit." The term "AAA" is used to evaluate the level of quality of counterfeit goods and to indicate to potential buyers how close the forgery is to the original item.[7]

The user retailed the items at 280.42 euros per unit and stressed that they were not stolen, thus not authentic products.

[5] Lutte contre la contrefaçon: un enjeu majeur de la pérennité des entreprises
[6] Unifab, Dossier de Presse
[7] You call yourself an Expert? The 3 Grades of Replicas You Must Know



Louis Vuitton Duffel Bag Superclone Grey

Type:	Physical	**280.42 EUR** per Bag	● **Kenza**	Level 126
Category:	Clothing + Jewelry		**Member since:**	2020-06-27
From:	United Kingdom of Great Britain		**# of Deals:**	203
Stock:	2		**Stealth:**	★★★★★
Sales:	0		**Quality**	★★★★★
Shipping to:	Show		**Communication:**	★★★★★

1 ADD TO CART

Description Terms & Conditions Feedback

Louis Vuitton Duffel Bag Superclone Grey

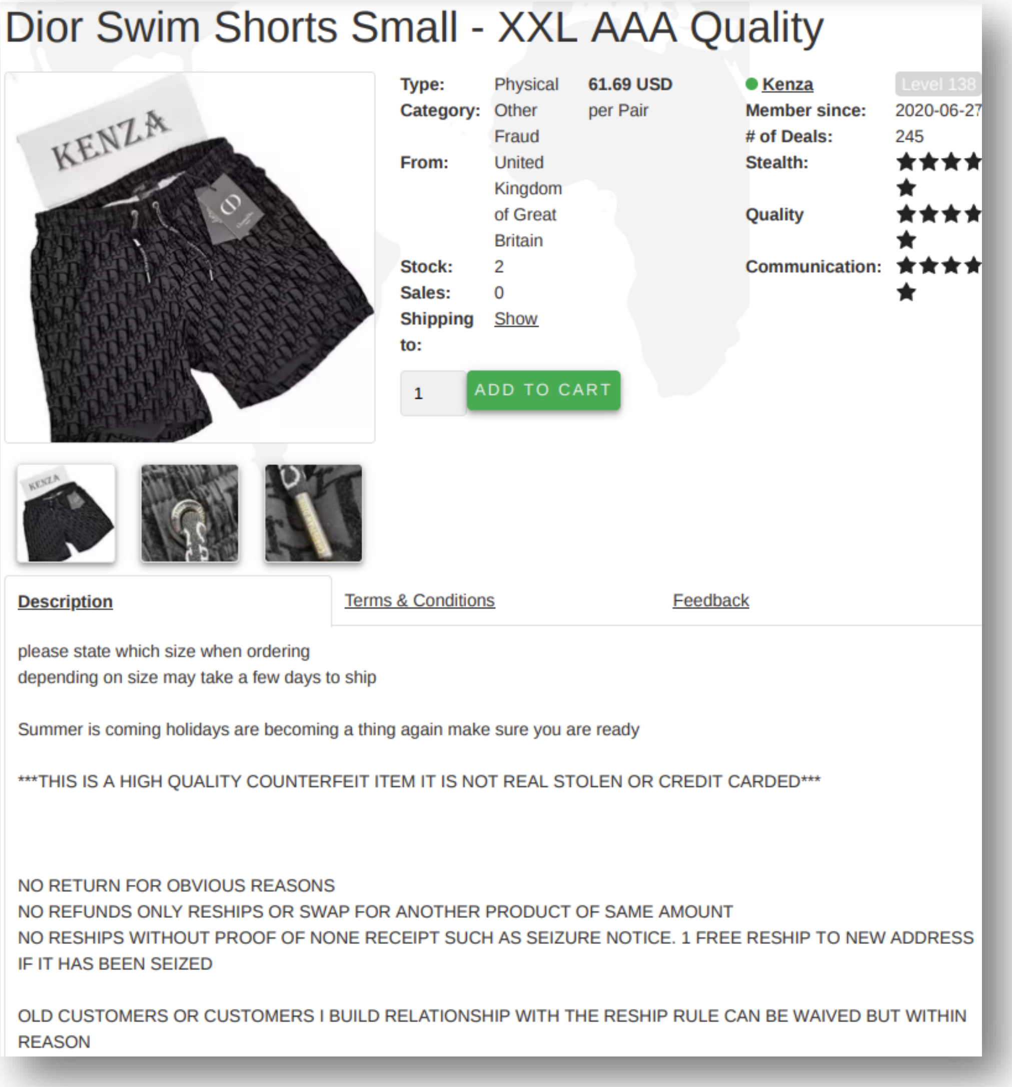
buy quick before they sell out when flights start opening up again

i know shipping is expensive blame brexit

This is a AAA grade counterfeit
this is not stolen
this is not carded
please stop asking

Versus Project Market post retrieved via KELA's Cybercrime Investigations platform

The same user also advertised Dior items such as the one below:



Dior Swim Shorts Small - XXL AAA Quality

Type: Physical
Category: Other Fraud
From: United Kingdom of Great Britain
Stock: 2
Sales: 0
Shipping to: Show

61.69 USD per Pair

● Kenza Level 138
Member since: 2020-06-27
# of Deals: 245
Stealth: ★★★★★
Quality ★★★★★
Communication: ★★★★★

1 ADD TO CART

Description Terms & Conditions Feedback

please state which size when ordering
depending on size may take a few days to ship

Summer is coming holidays are becoming a thing again make sure you are ready

THIS IS A HIGH QUALITY COUNTERFEIT ITEM IT IS NOT REAL STOLEN OR CREDIT CARDED

NO RETURN FOR OBVIOUS REASONS
NO REFUNDS ONLY RESHIPS OR SWAP FOR ANOTHER PRODUCT OF SAME AMOUNT
NO RESHIPS WITHOUT PROOF OF NONE RECEIPT SUCH AS SEIZURE NOTICE. 1 FREE RESHIP TO NEW ADDRESS IF IT HAS BEEN SEIZED

OLD CUSTOMERS OR CUSTOMERS I BUILD RELATIONSHIP WITH THE RESHIP RULE CAN BE WAIVED BUT WITHIN REASON

Branding strategies developed by luxury companies present luxury goods as rare and desirable items that are associated with quality, scarcity, and opulence. The wide availability of counterfeits, their low quality, and their affordability damage that image, which the brands use to justify the products’ higher costs.

Social Media Sources

Telegram

Private and encrypted social media channels such as Telegram pose an ideal platform for fraudsters who want to conduct illegal business and sell counterfeit goods anonymously. On Telegram, only users who are in someone's contact list can have access to their phone numbers, but users also have the option to hide their phone numbers from those in their contact list to ensure a higher level of privacy.[8] An additional way to remain anonymous while using Telegram is to register using a burner phone, a phone line that is purchased anonymously because it doesn't have a phone plan and isn't associated with its user's identity.

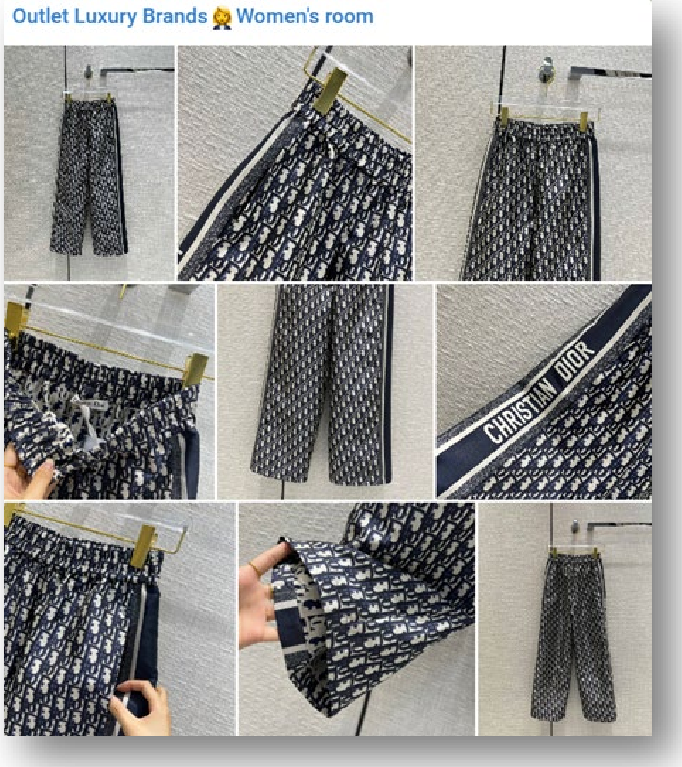
Telegram's moderation policies are described as more lenient than those of other platforms,[9] which contributes to making it attractive for cybercriminals.

Some channels can be particularly active, with dozens of new posts every day. Others are more discreet and post fewer pictures of brand logos but rather describe the goods available or state that potential buyers can submit requests and that the sellers will attempt to provide the requested items. Popular channels or groups may have several thousands of members or subscribers. Users can order items without having to join or subscribe, simply by checking the group's or channel's admin user ID and contacting them directly, if they don't want to have their own account associated with counterfeit groups.

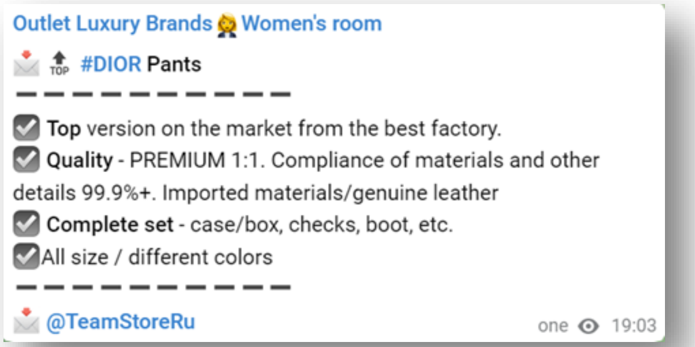
The example below is of Outlet Luxury Brands Women's Room, a Russian-language Telegram channel that sells counterfeit fashion items from a wide range of luxury brands including Chanel, Dior, Balmain, Celine and Louis Vuitton. The fraudsters who operate this channel claim that their products are in "compliance of materials and other details 99.9%" compared with the original items.

[8] How to Hide your Phone Number in Telegram

[9] Content Moderation Case Study: Telegram Gains Users But Struggles To Remove Violent Content (2021)



Outlet Luxury Brands 👸 Women's room



Outlet Luxury Brands 👸 Women's room

📩 🔝 #DIOR Pants

— — — — — — — — — —

☑ **Top** version on the market from the best factory.

☑ **Quality** - PREMIUM 1:1. Compliance of materials and other details 99.9%+. Imported materials/genuine leather

☑ **Complete set** - case/box, checks, boot, etc.

☑All size / different colors

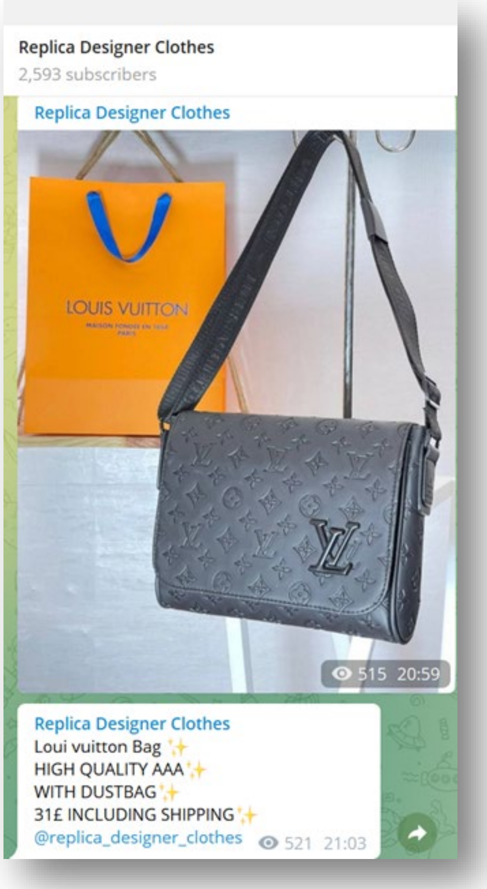
— — — — — — — — — —

📩 @TeamStoreRu

one 👁 19:03

Telegram post advertising Dior counterfeits (automatically translated from Russian)

Other channels also advertise fake designer items. For example, Replica Designer Clothes, which was created on June 24, 2022, sells clothes, shoes, and handbags similar to the following one:



Replica Designer Clothes
2,593 subscribers

Replica Designer Clothes

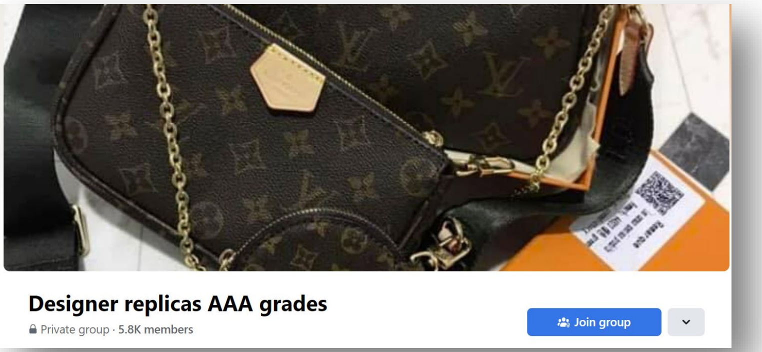
Replica Designer Clothes
Loui vuitton Bag ✨
HIGH QUALITY AAA ✨
WITH DUSTBAG ✨
31£ INCLUDING SHIPPING ✨
@replica_designer_clothes 521 21:03

Telegram post advertising Louis Vuitton counterfeits

The channel's operators describe this item as a Louis Vuitton bag of high quality (AAA). This product is presented with a branded carrier bag and comes with a dust bag. The bag is sold for 31 GBP which represents a fraction of the genuine item's market value.

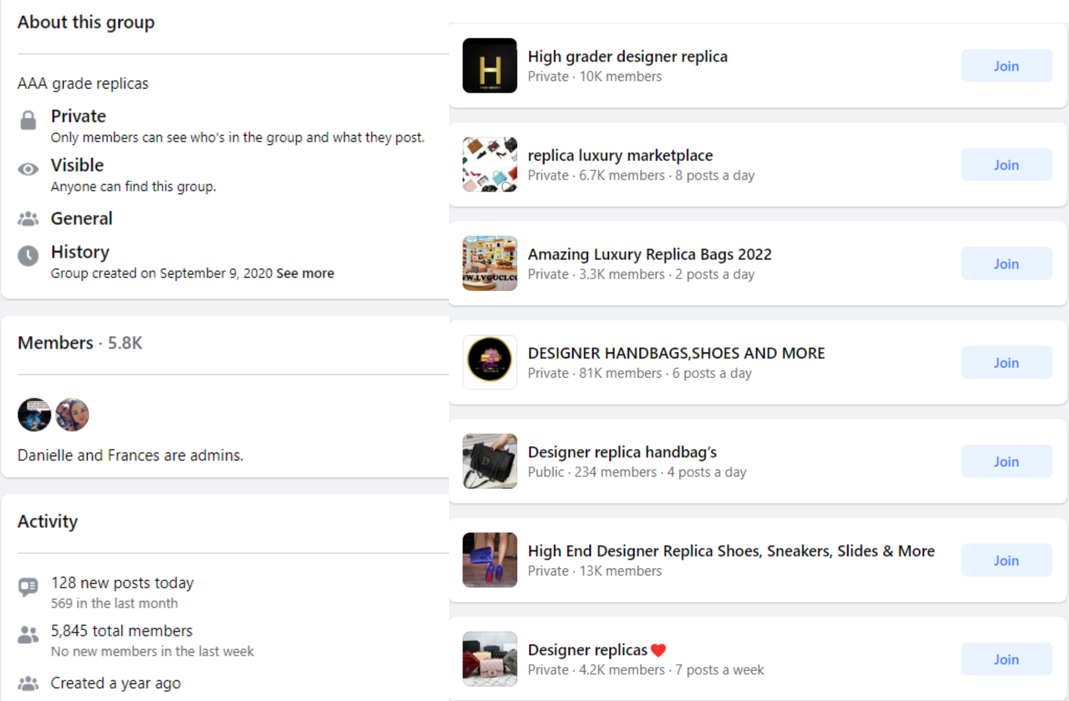
Facebook

Counterfeit luxury items are also available on Facebook groups where users advertise designer replicas. Counterfeit French luxury items can be purchased from resellers posting on these groups, which have several thousands of members and a few hundred new posts per day.



Designer replicas AAA grades

Private group · 5.8K members



About this group

AAA grade replicas

Private
Only members can see who's in the group and what they post.

Visible
Anyone can find this group.

General

History
Group created on September 9, 2020 **See more**

Members · 5.8K

Danielle and Frances are admins.

Activity

128 new posts today
569 in the last month

5,845 total members
No new members in the last week

Created a year ago

High grader designer replica
Private · 10K members

replica luxury marketplace
Private · 6.7K members · 8 posts a day

Amazing Luxury Replica Bags 2022
Private · 3.3K members · 2 posts a day

DESIGNER HANDBAGS,SHOES AND MORE
Private · 81K members · 6 posts a day

Designer replica handbag's
Public · 234 members · 4 posts a day

High End Designer Replica Shoes, Sneakers, Slides & More
Private · 13K members

Designer replicas ❤
Private · 4.2K members · 7 posts a week

On the left - a screenshot of the description of the Facebook group Designer replicas AAA grades. On the right - a screenshot of a list of several Facebook groups selling designer counterfeits.

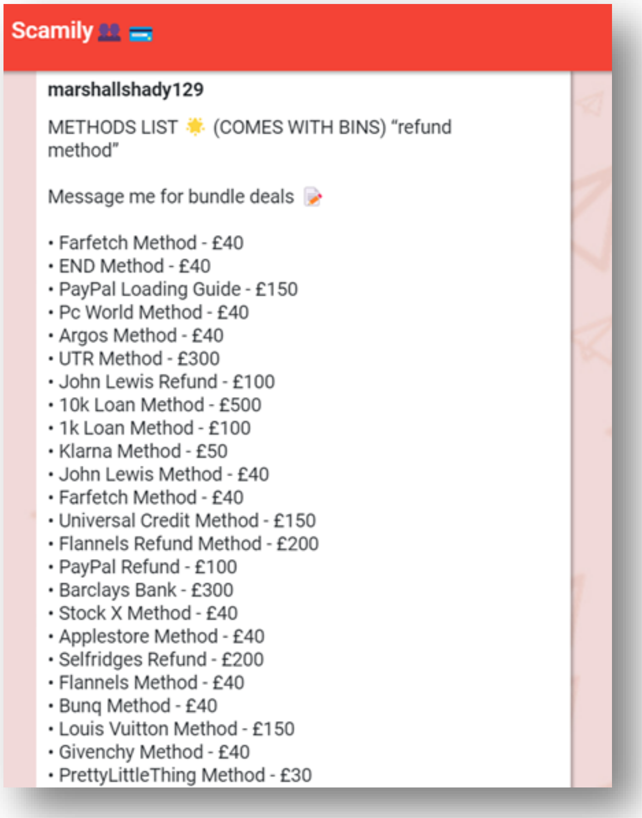
While most such groups are private, anyone can ask to join. They are less private and less secure than Telegram groups or encrypted channels.

Even if social media companies have anti-counterfeit policies and try to limit the number of channels selling illegal goods, it’s effortless for users to open such channels, operate them until they get closed down by moderators, and then create new ones and start their operations again.

The counterfeit industry causes hundreds of millions of euros in losses to luxury companies every year, in spite of regulators and law-enforcement agencies working to stop this underground business. High demand for luxury goods drives an ever-increasing level of offers that flourish across social media platforms and that isn’t likely to diminish any time soon because the sellers rarely have to face justice, as a large percentage of counterfeits are shipped from abroad and those seized at customs may be traced back to the sellers, however, getting the sellers arrested would require the cooperation of the authorities from the country they are based in. As a result, the sellers often can continue their online activities.

Refund Methods

Buying items online and finding ways to keep them while getting a refund is a type of fraud that is popular among online scammers, and they have been sharing and selling methods on how to carry out such scams. This type of scam is even more attractive when it comes to luxury items considering their higher value, which entails bigger refunds for online fraudsters. KELA observed these methods targeting luxury brands being sold in Telegram groups, as can be seen in the example below:



Scamily 👥 💳

marshallshady129

METHODS LIST ☀️ (COMES WITH BINS) “refund method”

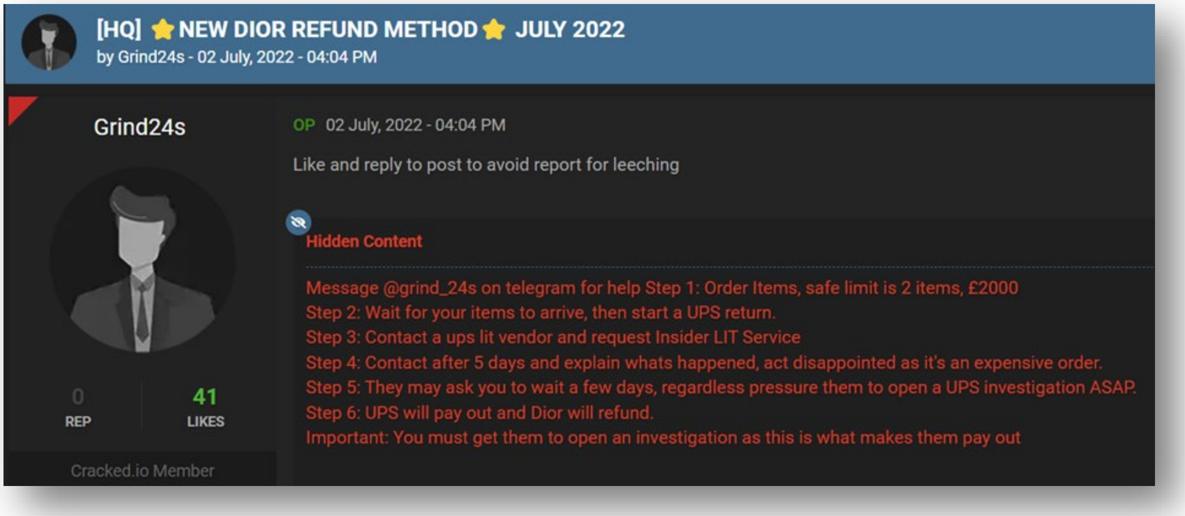
Message me for bundle deals 📝

- Farfetch Method - £40
- END Method - £40
- PayPal Loading Guide - £150
- Pc World Method - £40
- Argos Method - £40
- UTR Method - £300
- John Lewis Refund - £100
- 10k Loan Method - £500
- 1k Loan Method - £100
- Klarna Method - £50
- John Lewis Method - £40
- Farfetch Method - £40
- Universal Credit Method - £150
- Flannels Refund Method - £200
- PayPal Refund - £100
- Barclays Bank - £300
- Stock X Method - £40
- Applestore Method - £40
- Selfridges Refund - £200
- Flannels Method - £40
- Bunq Method - £40
- Louis Vuitton Method - £150
- Givenchy Method - £40
- PrettyLittleThing Method - £30

Refund methods for French luxury brands Louis Vuitton and Givenchy, for example, are available for 150 GBP and 40 GBP respectively. These and other refund methods typically consist of ordering an item from the retailer’s online shop, then claiming the item is damaged or didn’t arrive. If the scammer said the product was damaged, they pretend to send it back while sending only an empty box and demand a refund.

This type of fraud affects a large number of online retailers, and thus luxury companies that sell costly items tend to be targets of choice for online scammers, who see the potential for higher profits.

Other threat actors share their refund methods for free. A member of the Cracked forum named “Grind24s” posted a refund method for Dior that also involved the courier company UPS.



[HQ] ⭐ NEW DIOR REFUND METHOD ⭐ JULY 2022

by Grind24s - 02 July, 2022 - 04:04 PM

Grind24s

0 REP

41 LIKES

Cracked.io Member

OP 02 July, 2022 - 04:04 PM

Like and reply to post to avoid report for leeching

Hidden Content

Message @grind_24s on telegram for help Step 1: Order Items, safe limit is 2 items, £2000
Step 2: Wait for your items to arrive, then start a UPS return.
Step 3: Contact a ups lit vendor and request Insider LIT Service
Step 4: Contact after 5 days and explain whats happened, act disappointed as it's an expensive order.
Step 5: They may ask you to wait a few days, regardless pressure them to open a UPS investigation ASAP.
Step 6: UPS will pay out and Dior will refund.
Important: You must get them to open an investigation as this is what makes them pay out

Screenshot from a post from July 2, 2022 from the Cracked forum

The steps described above start with an online order of a Dior item, for a maximum amount of 2000 GBP, according to the advice from the fraudster. Upon receipt of the item, the customer should initiate a UPS return and request "insider LIT Service," wait five days before pretending that the ordered item was not received, and insist that UPS open an investigation. Such an investigation should result in the carrier having to pay the company from which the item was purchased – in this example, Dior – and in Dior making a refund to the customer. In cases such as these, the fraudsters also keep the items that they claimed not to have received.

Exposed Information

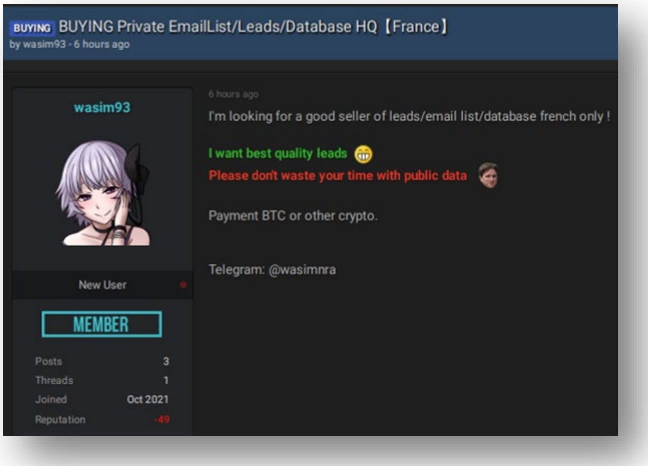
Luxury companies, and the retail sector in general, are also affected by cybercrime that stems from data exposure. Leaked data from retailers often include clients and/or employees' databases and exposed data from a company that could allow threat actors to attack it.

The private information of luxury brands' customers could, for example, allow threat actors to conduct targeted phishing campaigns or to carry out social engineering attacks. Luxury companies' customers are generally expected to be rather wealthy, which makes them prime targets for cybercriminals. And employee data could provide attackers with the means to compromise a company and access valuable information to conduct a whole range of malicious activities.

KELA's review of cybercrime underground sources identified chatter related to French data and specifically to data from French luxury companies.

Demand for databases

Threat actors often look for private information in cybercrime forums that they can use to conduct several types of scams or to gain illegal access to an online retailer account. Cybercriminals may search for data from a specific country, as can be seen with the example below from the now defunct RaidForums, where the user "wasim93" says they want to buy a "private email list/leads/database" and are only interested in French data.



BUYING BUYING Private EmailList/Leads/Database HQ【France】
by wasim93 - 6 hours ago

wasim93

New User

MEMBER

Posts	3
Threads	1
Joined	Oct 2021
Reputation	-49

6 hours ago

I'm looking for a good seller of leads/email list/database french only !

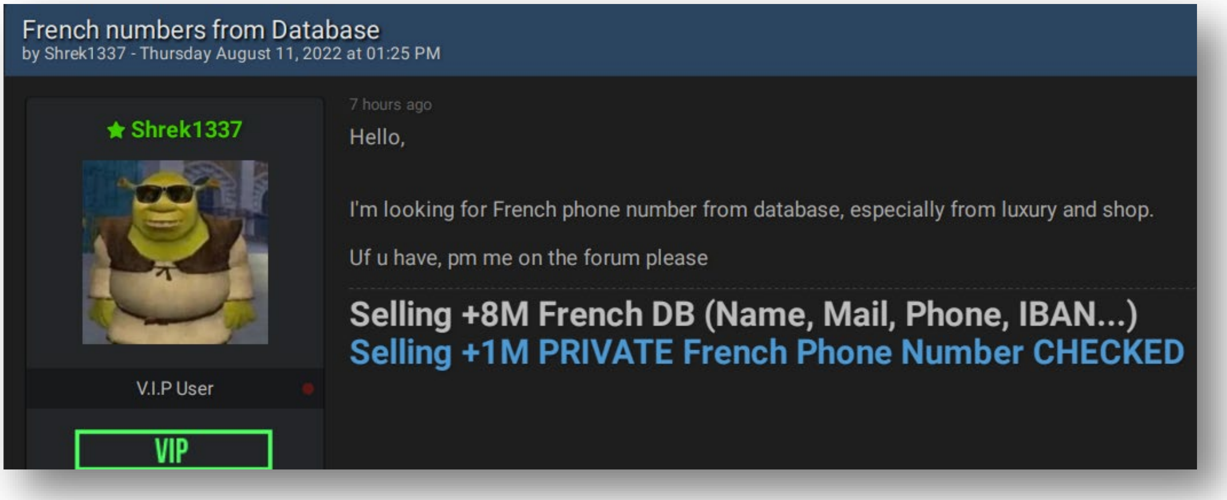
I want best quality leads 😁
Please don't waste your time with public data

Payment BTC or other crypto.

Telegram: @wasimnra

RaidForums post from October 19, 2021, retrieved via KELA's Cybercrime Investigations platform

A user operating under the moniker “Shrek1337” on BreachForums was spotted searching for French phone-number databases and specified they were particularly interested in luxury shops.



French numbers from Database
by Shrek1337 - Thursday August 11, 2022 at 01:25 PM

★ Shrek1337

V.I.P User

VIP

7 hours ago

Hello,

I'm looking for French phone number from database, especially from luxury and shop.

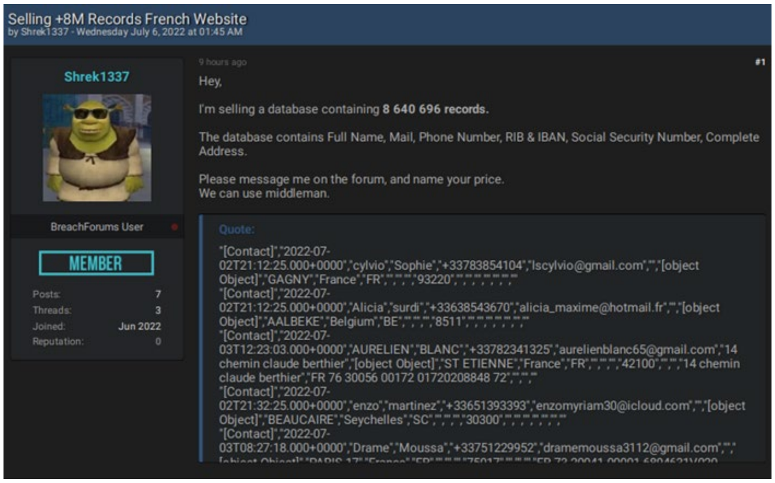
Uf u have, pm me on the forum please

Selling +8M French DB (Name, Mail, Phone, IBAN...)
Selling +1M PRIVATE French Phone Number CHECKED

BreachForums post from August 11, 2022, retrieved via KELA’s Cybercrime Investigations platform.

Offers of databases

French data was also found for sale in other cybercrime sources, similarly to the instance below where the same user, “Shrek1337,” offers for sale over 8 million records from a French website. As stated on the threat actor’s post, the database allegedly contains “Full Name, Mail, RIB & IBAN, Social Security Number, Complete Address.”



Selling +8M Records French Website
by Shrek1337 - Wednesday July 6, 2022 at 01:45 AM

Shrek1337

BreachForums User

MEMBER

Posts:	7
Threads:	3
Joined:	Jun 2022
Reputation:	0

9 hours ago #1

Hey,

I'm selling a database containing **8 640 696 records.**

The database contains Full Name, Mail, Phone Number, RIB & IBAN, Social Security Number, Complete Address.

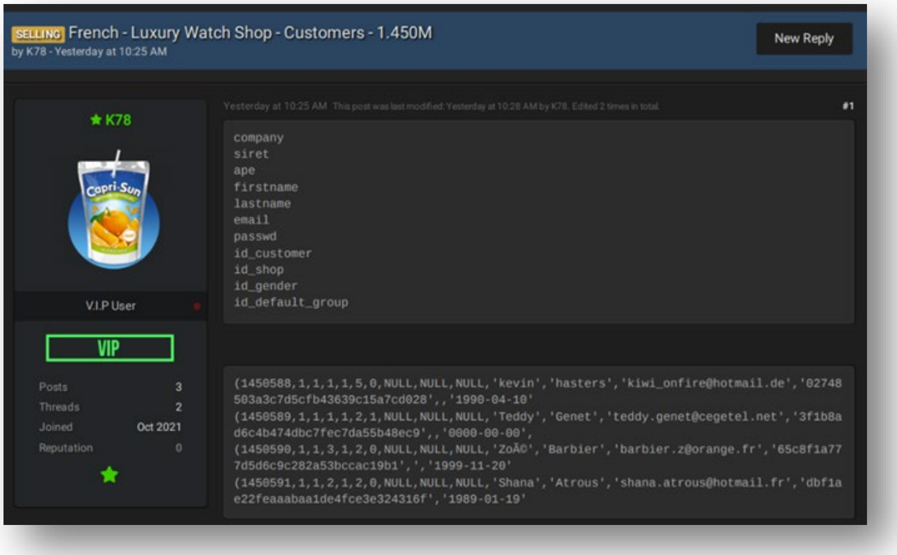
Please message me on the forum, and name your price.
We can use middleman.

Quote:

```
"[Contact]","2022-07-
02T21:12:25.000+0000","cylvio","Sophie","+33783854104","lscylvio@gmail.com","","[object
Object]","GAGNY","France","FR","","","","93220","","","","","","",""
"[Contact]","2022-07-
02T21:12:25.000+0000","Alicia","surdi","+33638543670","alicia_maxime@hotmail.fr","","[object
Object]","AALBEKE","Belgium","BE","","","","8511","","","","","","",""
"[Contact]","2022-07-
03T12:23:03.000+0000","AURELIEN","BLANC","+33782341325","aurelienblanc65@gmail.com","14
chemin claude berthier","[object Object]","ST ETIENNE","France","FR","","","","42100","","","14 chemin
claude berthier","FR 76 30056 00172 01720208848 72","",""
"[Contact]","2022-07-
02T21:32:25.000+0000","enzo","martinez","+33651393393","enzomyriam30@icloud.com","","[object
Object]","BEAUCAIRE","Seychelles","SC","","","","30300","","","","","","",""
"[Contact]","2022-07-
03T08:27:18.000+0000","Drame","Moussa","+33751229952","dramemoussa3112@gmail.com","",
[object Object]","PARIS 17","France","FR","","","","75017","","","","FR 73 20041 00001 6804621V020
```

BreachForums post from July 5, 2022, retrieved via KELA’s Cybercrime Investigations platform

Threat actors have also been observed selling data from a set industry and country. Databases from luxury companies can be found for sale in underground forums. One such instance was retrieved from RaidForums, where a user named “K78” advertised a database from a French luxury watch shop allegedly containing 1.45 million records with clients’ full names, email addresses, passwords, and dates of birth.



French - Luxury Watch Shop - Customers - 1.450M
by K78 - Yesterday at 10:25 AM

★ K78

Posts 3
Threads 2
Joined Oct 2021
Reputation 0

Yesterday at 10:25 AM This post was last modified: Yesterday at 10:28 AM by K78. Edited 2 times in total. #1

```
company
siret
ape
firstname
lastname
email
passwd
id_customer
id_shop
id_gender
id_default_group
```

```
(1450588,1,1,1,1,5,0,NULL,NULL,NULL,'kevin','hasters','kiwi_onfire@hotmail.de','02748
503a3c7d5cfb43639c15a7cd028',,'1990-04-10'
(1450589,1,1,1,1,2,1,NULL,NULL,NULL,'Teddy','Genet','teddy.genet@cegetel.net','3f1b8a
d6c4b474dbc7fec7da55b48ec9',,'0000-00-00',
(1450590,1,1,3,1,2,0,NULL,NULL,NULL,'ZoÃ©','Barbier','barbier.z@orange.fr','65c8f1a77
7d5d6c9c282a53bccac19b1',',','1999-11-20'
(1450591,1,1,2,1,2,0,NULL,NULL,NULL,'Shana','Atrous','shana.atrous@hotmail.fr','dbf1a
e22feaaabaa1de4fce3e324316f','1989-01-19'
```

RaidForums post from October 22, 2021, retrieved via KELA’s Cybercrime Investigations platform

Threat actors may attempt to use the data acquired to gain access to the client’s online accounts and make illegal purchases or try to retrieve potentially stored payment information. Such databases may also be used for phishing campaigns.

While a wide range of information can be leaked from a company, credentials that might be abused to gain access to its online platforms, such as clients’ accounts but especially employee-related platforms or servers, are particularly valuable for cybercriminals.

Leaked Credentials

Leaked credentials are leaked email logins automatically collected by KELA’s Cybercrime Intelligence platform, with and without passwords, which are referred to as leaked credentials. Corporate leaked credentials could allow a threat actor to access employees’ work emails and impersonate employees to gather critical business data or defraud the organization and its vendors, clients, or other employees.

KELA reviewed the leaked credentials pertaining to the 10 French companies investigated in this research, which were collected from leaked databases that were retrieved and ingested in the last few years. Once the data is leaked, it’s often shared multiple times, as threat actors tend to repost databases in other forums in order to acquire forums’ credits or reputation points, and may sometimes also attempt to resell them. Therefore, KELA decided to evaluate the companies’ overall exposure, rather than to set a limited time scope.

The analysis uncovered 42,800 leaked-credential detections for the reviewed domains. Out of these, 31,335 were found to be unique. The “non-unique” ones are credentials that have been exposed in more than one data breach. These credentials have been exposed due to third-party breaches that have been shared in cybercrime hacking sources. The credentials gathered were exposed in data breaches that occurred from 2012 to 2022. The data collected includes leaked credentials of five brands’ CEOs and of one brand owner, some with passwords, either hashed or in plain text. Some of these CEOs’ credentials were leaked in several breaches, and others also have several email addresses that appear in multiple data breaches.

Out of the leaked credentials collected, 8.3% included plain-text passwords, which could have been used to abuse the corporate’s email addresses and carry out illegal activities. About 3.5% had encrypted passwords, such as MD5 or SHA512, and the remaining 88% didn’t have any passwords. Even the corporate credentials that weren’t leaked with passwords could still be exploited by threat actors to conduct phishing campaigns, or passwords could be acquired using brute-force techniques.

Top Breaches

The top three data breaches observed contained about 80% of the leaked credentials from the French luxury companies reviewed.

- **Apollo Breach**

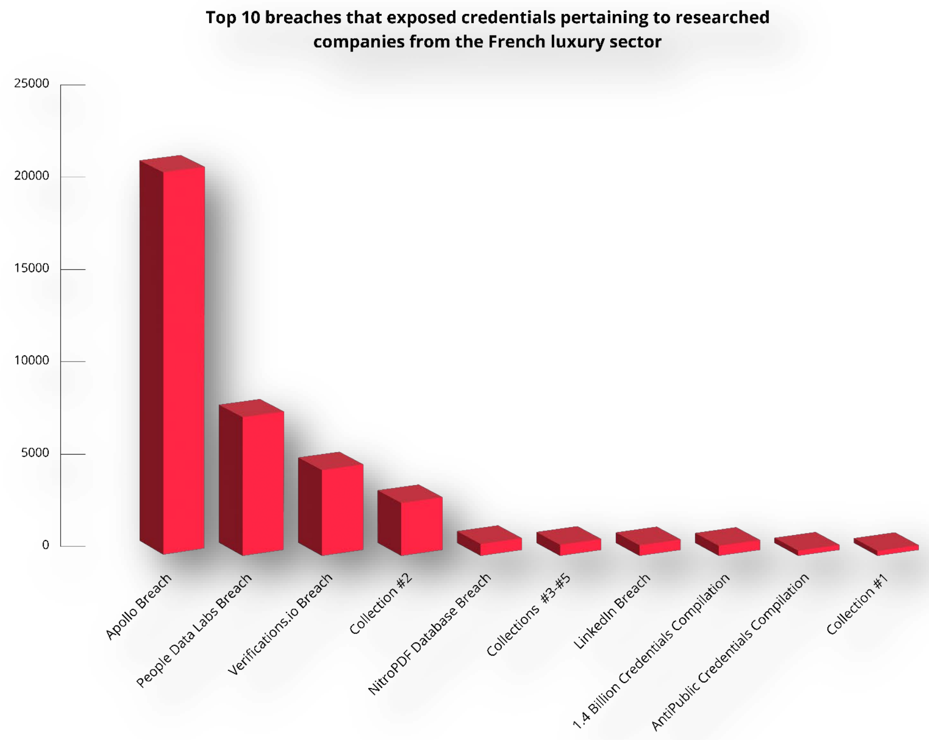
  Just above half of the leaked credentials collected (51%) were from the Apollo breach. Apollo is a sales engagement start-up, which was originally breached in July 2018, but the data was only shared in November 2020. The data leak exposed over 147 million user records and included users' email addresses, full names, phone numbers, physical location, and employment information. Based on a review of data samples from the Apollo breach, the professional data found was likely collected by the company from LinkedIn profiles.

- **People Data Labs**

  Of the leaked credentials analyzed, 18.5% were found to have originated from the breach of People Data Labs, a data enrichment platform. The leaked data included email addresses, phone numbers and social media profiles. The leak occurred in October 2019 when security researchers found 1.4 billion personal records on an unsecured Elastic server. In October 2020, 416 million records allegedly originating in the leak were shared for download on a cybercrime forum.

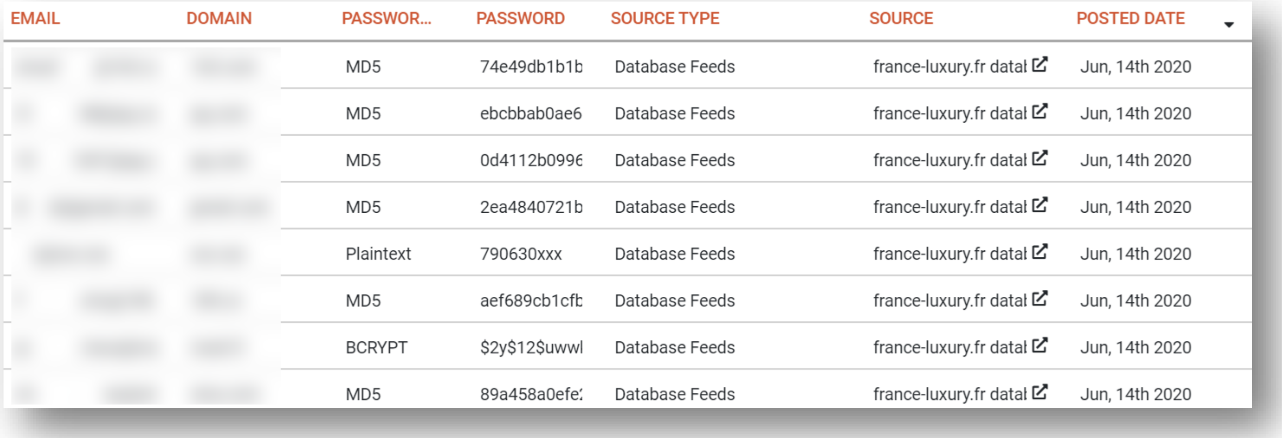
- **Verification.io**

  The breach of the email verification platform verifications.io exposed 11.5% of the leaked credentials. In February 2019, verifications.io suffered a data breach that exposed 763 million consumer records, including email addresses, names, IP addresses, phone numbers, and other personal information.


Top 10 breaches that exposed credentials pertaining to researched companies from the French luxury sector

Collections 1 through 5 in the graphic above (shared in 2019), as well as the 1.4 Billion and AntiPublic credentials compilations (shared in 2017 and 2019), are data dumps made up of credential compilations aggregated from multiple data breaches that are not unique but may still pose a threat, since users don’t update their passwords regularly and these data dumps are constantly being shared in forums.

As for databases focused on the researched sector, KELA also observed the data breach of the site france-luxury[.]fr. The site publishes blogs, reviews, and recommendations about the French luxury sector on topics including fashion, jewelry, hotels, gastronomy, and yachts. The database includes about 13,500 credentials and was retrieved by KELA in June 2020. While the site breached isn’t a luxury company itself, its main purpose is to discuss and review products and services from the luxury sector in France.



EMAIL	DOMAIN	PASSWOR...	PASSWORD	SOURCE TYPE	SOURCE	POSTED DATE
[redacted]	[redacted]	MD5	74e49db1b1b	Database Feeds	france-luxury.fr datal	Jun, 14th 2020
[redacted]	[redacted]	MD5	ebcbbab0ae6	Database Feeds	france-luxury.fr datal	Jun, 14th 2020
[redacted]	[redacted]	MD5	0d4112b0996	Database Feeds	france-luxury.fr datal	Jun, 14th 2020
[redacted]	[redacted]	MD5	2ea4840721b	Database Feeds	france-luxury.fr datal	Jun, 14th 2020
[redacted]	[redacted]	Plaintext	790630xxx	Database Feeds	france-luxury.fr datal	Jun, 14th 2020
[redacted]	[redacted]	MD5	aef689cb1cfb	Database Feeds	france-luxury.fr datal	Jun, 14th 2020
[redacted]	[redacted]	BCRYPT	$2y$12$uwwl	Database Feeds	france-luxury.fr datal	Jun, 14th 2020
[redacted]	[redacted]	MD5	89a458a0efe:	Database Feeds	france-luxury.fr datal	Jun, 14th 2020

The database was leaked as part of the Cit0day website collection. Cit0day was a website that indexed and collected previously leaked databases and made them available to its members against a subscription fee. The website contained databases from 23,600 websites that were either new or previously shared.[10]

Compromised Accounts

Compromised accounts are logins and passwords that pertain to online accounts, including tools and software used in a corporate environment, and that could allow an attacker to access internal systems. Compromised accounts are regularly offered for sale on underground automated botnet markets.

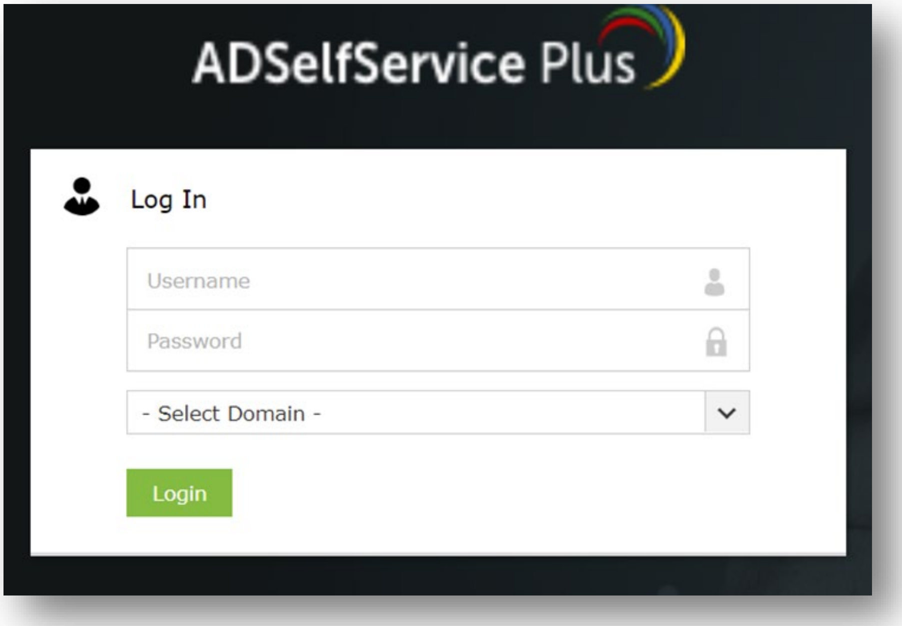
KELA analyzed the compromised accounts of the researched French luxury companies and detected 1,700 instances that were offered for sale on several automated botnet markets. Credentials stolen from infected devices, such as smartphones and computers, were put up for sale on these botnet markets. Often the credentials were logins and passwords for online accounts that belong to a company's clients — or to its employees or third-party vendors' employees, which could offer threat actors a point of access into the company's network.

[10] https://www.bitdefender.com/blog/hotforsecurity/data-breach-saga-what-you-need-to-know-about-the-cit0day-data-leak

Logins and passwords for customer online portals constitute the vast majority of compromised accounts collected. They often give access to online shopping accounts that store a wide range of user data, including names, dates of birth, addresses, phone numbers and payment information such as credit card details. Often, luxury companies offer personalized services to their customers. To that end, they allow users to save their orders, wish lists and recommendations, and to make appointments with specific stores or to keep track of their items sent to "care services" for repair or maintenance.

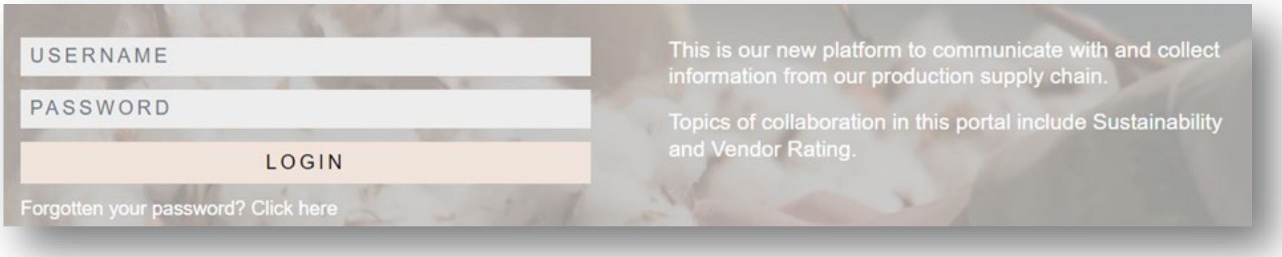
KELA's monitoring of botnet markets uncovered compromised accounts of employee portals at several of the top French luxury companies, which could be purchased and accessed by cybercriminals to use as initial access to carry out an attack.

Within these highly sensitive resources, KELA identified some accounts associated with the ADSelfService Plus platform, which allows administrators to control and enable password resets and to unlock accounts for employees. If compromised, this portal would allow malicious actors to log into the account of a user and potentially reset passwords to access additional accounts, possibly including some with admin access in order to pivot into the company's network.



ADSelfService Plus' user login page, which could be accessed using login data purchased from Genesis, RussianMarket, and TwoEasy.

An additional example of a resource detected by KELA that could be compromised and may pose a threat to one of the companies we looked into, is a third-party vendor portal.



This is our new platform to communicate with and collect information from our production supply chain.

Topics of collaboration in this portal include Sustainability and Vendor Rating.

A vendor portal that could be compromised using credentials bought from RussianMarket

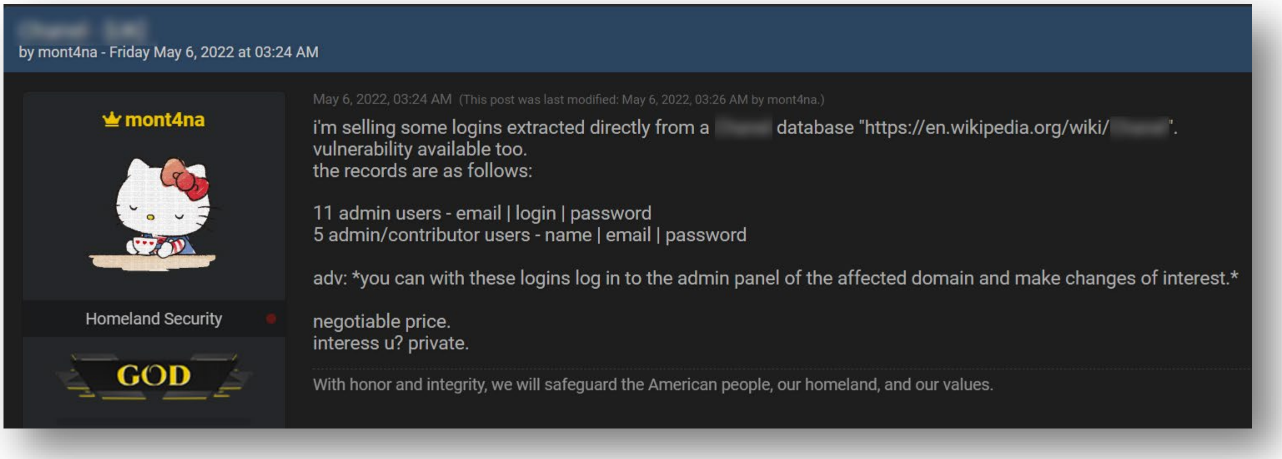
Purchasing credentials for this platform could allow attackers to gain information about a company's supply chain, which could enable them to compromise it, communicate with other third-party vendors, and attempt to conduct scams by, for example, issuing bills to the vendors and changing the recipient's bank credentials to those of the attackers.

Network Accesses

Initial network accesses are entry points into a company's network and may be abused by cybercriminals to extract proprietary data, conduct espionage campaigns or carry out ransomware attacks. These accesses can be found for sale on underground forums. While the Initial Access Brokers rarely provide the names of the entities to whose network they're selling access, they often provide some information, which might include the victim's sector, country, and revenue.

Based on information shared by these actors, KELA detected initial access for 67 French companies that were put up for sale between August 2021 and August 2022, including three from the retail sector. Once put up for sale, network accesses tend to be sold in a matter of days. KELA's research focused on offers from the last 12 months to reflect the current threats faced by French luxury companies and more broadly by the retail sector in France.

Below is an example of a luxury company that was detected during the research period. On May 6, 2022, the actor operating under the moniker “mont4na,” also known as “pumpedkicks,” advertised admin-level account logins belonging to an iconic French luxury fashion brand, which they claimed to have extracted using a vulnerability that they also offered to sell. According to the actor’s post, the logins provide access to the affected domain’s admin panel.



[redacted]
by mont4na - Friday May 6, 2022 at 03:24 AM

May 6, 2022, 03:24 AM (This post was last modified: May 6, 2022, 03:26 AM by mont4na.)

i'm selling some logins extracted directly from a [redacted] database "https://en.wikipedia.org/wiki/[redacted]".
vulnerability available too.
the records are as follows:

11 admin users - email | login | password
5 admin/contributor users - name | email | password

adv: *you can with these logins log in to the admin panel of the affected domain and make changes of interest.*

negotiable price.
interess u? private.

With honor and integrity, we will safeguard the American people, our homeland, and our values.

Screenshot of mont4na’s offer posted on BreachForums

Ransomware Attacks

KELA recorded 290 ransomware attacks targeting French companies from all sectors, 24 of which belong to the consumer and retail sector. However, while none of the ransomware victims observed during the scope of this research belonged to the luxury sector, some of the victims that paid the ransom and were not made public may have belonged to that industry. Additionally, some of the recorded compromised companies may have had business relationships with luxury companies, which in turn may have been compromised by ransomware attacks targeting their third-party vendors, partners, or clients.

The data was collected from ransomware blogs, data leak sites, negotiation portals, and public reports from 2020 to 2022, a period during which ransomware groups’ activity drastically increased.

It is important to note that some victims may have paid the ransom requested by threat actors and thus wouldn't appear on any of the sources listed above. In addition, it's not always possible to identify victims from negotiation portals. Thus, the actual number of French entities targeted by ransomware attacks may be higher than previously stated.

Conclusion

The luxury industry is one of France's economic pillars, as it drives the nation's exports. Leading luxury brands face growing cyber threats as online criminals try to monetize clients' data or to exploit employees' credentials as initial points of access. Companies must educate their employees and apply security measures. Third-party suppliers, vendors and partners also represent a threat, therefore luxury brands must track and secure their supply chains.

Based on the research, organizations in France, and globally, should ensure to continually:

- Train all employees and key individuals on safely using their credentials and personal information online. This cyber training should specifically include how to identify suspicious activities, such as possible scam emails or unusual requests from unauthorized individuals or email addresses. The human factor plays a significant role in an organization's cybersecurity. The larger the organization, the bigger chance of threats – therefore, creating such mandatory cybersecurity training across all these organizations would significantly reduce the chances that they would be compromised due to an employee's mistake.
- Consider implementing a VPN/WAF/2-step verification practice on the organization's clients, employees, and other internal portals to prevent unauthorized access to accounts.
- Enforce a periodical password change among the organization's employees and customers (the password should be new and different from any other passwords previously or currently utilized by the compromised users for any existing service or platform).
- Invest in regular vulnerability monitoring and patching. Due to the increased use of digital systems and ongoing updates of technologies, vulnerabilities in an organization's network are constantly going to rise. These organizations must invest in regular monitoring of their entire network infrastructure to ensure that any possible entry points for initial access brokers or other network intruders are immediately blocked.

- Monitor your assets to automatically detect your most relevant threats emerging from the cybercrime underground. Nowadays, every organization – private or government, small, medium, or large, is constantly at risk due to the ever-growing cybercrime ecosystem. Cybercriminals continually search for new opportunities to monetize the data they obtain. They are active in the hardest-to-reach corners of the cybercrime underground and organizations are constantly in need of defeating them. Constant automated and scalable monitoring of an organization’s assets could significantly improve maintaining a reduced attack surface, ultimately helping organizations prevent possible attempts of cyberattacks against them. For example, having detected leaked credentials or compromised accounts, the company can close unauthorized access and investigate the incident to prevent their use in additional targeted attacks.
- Constantly monitor the cybercrime landscape in general to discover recent trends and threats. Attackers develop methods to abuse algorithms, i.e., to commit refund fraud. Knowing the latest tactics and fraud trends may allow a company to address this evolving threat more adequately and decrease financial losses.