GROUP-IB STUDY: RELEVANT CYBERTHREATS TO PERFUME BRANDS IN 2019

group-ib.com

CONTENTS

01 ABSTRACT

THE STUDY CONTAINS:

Results of research into the online counterfeit perfumes market and online fraud

Recommendations for perfume manufacturers on how to respond to such violations

AIM OF THE STUDY:

To examine methods of abusing perfume companies' brands and popular products

To estimate the extent and monetary equivalent of counterfeits on sale

The distribution of counterfeited perfumes is a threat to targeted brands because it poses the risk of dilution — i.e. the loss of premium status and a strategically defined market niche. As a result, threat actors' abuse of perfume brands for profit may lead to decreased demand and customer trust.

Mass migration of customers and sellers to online resources takes the issue of brand security to a new level. Any transition to e-commerce entails an increased risk of digital fraud and cyberattacks.

Fraudsters actively use all available online channels to distribute counterfeited perfumes or attract traffic. While manufacturers compete against each other by developing new perfume formulas and taking responsibility for the quality of their products, fraudsters feed off their names, proven quality, and popularity.

The distribution of counterfeits is not the only danger posed by fraudulent resources that abuse brands. They also put the reputation of brand owners at risk and significantly affect their revenues by causing losses in profits.

Considering the extent of the problem, Group-IB's Digital Risk Protection team analyzed distribution channels and the volume of counterfeited perfume products distributed online. During their research, Group-IB's Digital Risk Protection experts analyzed hundreds of resources, including:

— domain names

— mobile apps

— social media pages

— resources designed for selling products under the names of famous brands

Having collected detailed information, Group-IB's Digital Risk Protection team focused only on the resources that appeared to sell counterfeits and analyzed the online counterfeit perfumes market.

02 RESEARCH METHODOLOGY

Selection:

5

largest perfume manufacturers

Data was obtained by monitoring open sources on the Internet and the Deep Web.

What we analyzed:

- distribution and traffic attraction methods
- platforms for selling counterfeits

For our research, we chose the giants, i.e. brands that are well-known worldwide. Their target audience is the entire international market.

Subjects

We analyzed mentions and posts about the sale of perfumes in both the Russian- and English-speaking parts of the Internet.

The following types of resources were covered:

- Yandex and Google search engines
- social media
- online stores
- relevant forums
- online bulletin boards
- Deep Web

Specifics

Group-IB specialists analyzed links between registration and contact data, IP addresses, and domain names, then identified what the analyzed resourced were affiliated with.

Limitations:

It is important to note that advertisements carry certain limitations that impact the study results. It is impossible to verify the following:

- product availability and advertisement accuracy
- product origin
- documents confirming product authenticity and sale legality

All quantitative estimations of the turnover of counterfeited goods are approximate. The lack of accurate information does not allow for a full picture of shadow processes and volumes.

03 EXTENT OF VIOLATIONS ON VARIOUS RESOURCES

Brand abuse platforms

Fraudulent resources emerge and disappear every day. Most are part of networks, and their design and specific characteristics are identical to those of the original brands.

We singled out three categories of fraudulent resources that pose the biggest threat to brands:

1. Resources dedicated to a specific brand

Websites that fully or partially copy official resources, with prices and contact details changed.

2. Resources dedicated to a specific product category

Resources with various products of the same type. These websites usually offer the most popular products within one product segment.

3. Multibrand and multicategory resources

Resources of this type are disguised as regular online stores and create an illusion of large-scale sales, thereby misleading customers, who might not be aware that they could fall victim to fraud.

HIGH

threat level

> 6 000

resources with names similar to those of perfume companies

Domain names

Group-IB’s Digital Risk Protection specialists discovered a high number of domain names that were similar to official ones. Such domains can be used for fraud purposes.

Not all the resources contained illicit content, however. For instance, out of all domains discovered while investigating one perfume company, 1,500 were “clean” (i.e. they had no content at all) and only one was not. However, this does not exclude the possibility of illegal content appearing on them at some point.

How fraudsters use similar-sounding domain names

Advertise their own services

Fraudsters mimic famous brands to promote their websites and attract traffic.

Pose as partners of famous brands

Fraudsters abuse a company’s logo or name to demonstrate their partnership, which in reality does not exist. Their poor services or even lack thereof then become associated with the original company, which in turn could lead to claims, customer enquiries, and even reputational damage.

Post inaccurate information

False information can mislead the original manufacturer’s potential customers and employees. Moreover, any counterfeits can be dangerous to health.

HIGH

threat level

35

mobile apps
on unofficial stores

Mobile apps

There are many mobile applications that can use (or not) the names and trademarks of brands.

Why unofficial mobile apps are dangerous

Risk of malware infection

Infected devices can transfer all information to threat actors, who gain access to the devices and steal users' personal data.

Mislead customers

Unofficial apps can have no updates for a long time or contain false or outdated information, which can entail health risks.

Inaccurate information

False information can mislead the original manufacturer's potential customers and employees. Moreover, any counterfeits can be dangerous to health.

HIGH

threat level

> 3 000

groups and accounts that,
in addition to names, use
perfume companies' identities
and sell "their" products.

Social media

Group-IB's Digital Risk Protection experts analyzed various social media groups and accounts that use perfume companies' and popular perfumes' identities and sell "their" products.

Their overall audience is more than two million people, which makes it clear that these platforms are a serious threat to companies' reputation.

In addition, we identified active social media groups and accounts that used the identities of perfume companies, both multi- and mono-brand ones

46	22	8

Number of social media groups
that target one brand

HIGH

threat level

**5,000-
10,000**

product-selling websites
per brand

Online stores

An analysis of posts that advertised counterfeited perfumes showed that most of them were sold on aggregators. Fraudsters actively use multibrand websites because it is easy and cheap to create them and attract traffic. The popularity of perfume only plays into their hands.

HIGH

threat level

1,800 - 20,000

объявлений приходится на один бренд

Online bulletin boards

The search covered Russian and international online bulletin boards:

- Avito — 9,150 posts
- Tiu — 11,150 posts
- Youla — 11,000 posts
- AliExpress —
- Amazon — 970 posts
- eBay — 15,450 posts
- DHGate and others

HIGH

threat level

> 3,600

messages about selling perfumes in 2019

Underground forums

Underground forums are used for selling products with brand names and advertising existing fraudulent resources (mainly in comments).

Some sellers distribute their products on several forums at once. There were also wholesale offers that mentioned multiple brands.

04

METHODS OF DISTRIBUTING PERFUME AND ATTRACTING TRAFFIC

User searches before purchases are made are an ideal time for fraudsters as this is the easiest stage for them to attract a potential buyer with a lucrative offer. Costs for fraudsters are minimal since regardless of the promotion method they choose, it will still produce results and bring profit.

An analysis of search queries revealed that there were tens of thousands of product-selling websites, including online bulletin boards and social media accounts and groups. In addition to search queries, search engines show contextual ads, which can mislead inexperienced users.

Ads

Fraudsters use various channels to attract shoppers to their resources:

- contextual advertising
- targeted bulk text messaging
- bulk messaging in messaging apps

These activities have a significant impact on the target audience’s attitude to brands and lead to reputational losses. Additional focus should be placed on ads that promote counterfeited perfumes in comments and on social media.

05 POTENTIAL DAMAGE

According to Data Insight, the conversion of online stores, calculated as the ratio of the number of orders to the number of visitors per month, is 4.4%.

Group-IB's Digital Risk Protection specialists calculated the potential damage to perfume companies from the sale of counterfeits on official Russian online stores.

The average basket price for an order of perfumes belonging to famous brands that we analyzed in the study ranges from $47.40 to $152.70.

Average basket price	$47.40	$152.70
Number of online stores	6,300	10,000
Monthly turnover	**$306,485**	**$1,532,429**

Losses were calculated using the following formula:

LOSSES = (average basket price × conversion × number of monobrand resources × average number of visitors + average basket price × conversion × number of multibrand resources × average number of visitors × average number of users interested in a particular product) × percentage of counterfeited perfumes

According to our estimates made using the formula above, the yearly volume of trade in counterfeits affecting the five perfume brands that we analyzed ranges from **$56.7 million to $344.7 million.**

Such large volumes involve almost no cost for the fraudsters as these online counterfeit distribution channels are free and easy to use.

06

GROUP-IB'S RECOMMENDATIONS FOR PERFUME COMPANIES

Conduct primary monitoring of the information field

The main goal is to assess the scale of the problem (number of violations) and determine high-priority sources. Primary monitoring will also indicate whether you need to take response measures. Even if there are currently no violations, it does not guarantee that they will not happen in the future. Some violations are temporary while others can be detected only through an in-depth analysis of information.

Implement a relevant monitoring system

Knowing the situation at the points of sale of counterfeited products requires systematic monitoring of the online space. The aim is to determine the scope of work to eliminate violations.

It is important that a monitoring system takes the interests of customers into account and analyzes the results of previous monitoring. To do so, it is crucial to use relevant user queries and search within the most popular sources among buyers.

Raise customer awareness

Buyers are not always well-informed about the manufacturing processes used by brands and differences between original and counterfeited products. Most people are easy to mislead. It is therefore crucial to organize awareness campaigns to educate potential customers.

GROUP IB

Group-IB is an international company that specializes in preventing and investigating cybercrime and online fraud using high technology.

Unique cyber intelligence data and proprietary solutions for tackling cybercrime are at the core of the company's **Digital Risk Protection** service. The continuous development of Group-IB's crime detection mechanisms has helped protect more than 200 Russian and international brands.

Moderator accounts on social media and close relationships with large platforms ensure that administrators promptly process the Digital Risk Protection team's requests to remedy breaches.

GARTNER IDC FORRESTER

Threat Intelligence, which is at the core of the Digital Risk Protection system, has been recognized as one of the best in its class by Gartner (2015), IDC (2016), and Forrester (2017).

FIRST TI

CERT GIB is an accredited member of international communities of security response teams such as FIRST and Trusted Introducer. This means that Group-IB is able to quickly block dangerous online resources worldwide.

IACC

Group-IB is recognized as a Competent Security Organization by the Coordination Centre for TLD RU and is a partner of the Foundation for Internet Development and part of the International AntiCounterfeiting Coalition (IACC).

17 YEARS

of experience in cybercrime investigation and analysis

1200+

successful investigations worldwide

Learn more about Group-IB's Digital Risk Protection

group-ib.com/digital-risk-protection
info@group-ib.com