May 2016

Andrea Stroppa, head of research

Daniele di Stefano, head of engineering

Bernardo Parrella, editor

Social media and luxury goods counterfeit: a growing concern for government, industry and consumers worldwide

Summary

1. Introduction 3
2. Fake luxury items proliferating online 5
3. Global counter-strategies…going nowhere? 8
4. Bots and AI as tools for online illicit trade 9
5. In search of 'legitimate' sellers of counterfeit goods 11
6. Key stats and features of fake accounts 15
7. Profile keywords and posting techniques 17
8. IM apps as top communication tools 21
9. Instagram spam-bot activities 25
10. Fraud and counterfeit activities on the web 26
11. Top countries involved 31
12. Top counterfeit brands 32
13. Illicit account activities 34
14. Interesting data about botnets 40
15. Illicit posts and hashtag search 42
16. The need for advanced detection systems 45
17. A difficult law-enforcement issue for Instagram 46
18. Conclusion 49

1. Introduction

The global economic impact of counterfeiting and piracy trade is skyrocketing. A multi-billion dollar underground economy, with hundreds of billions of dollars of counterfeit products being produced every year, has emerged in the last two decades. Today, counterfeit and pirated goods can be found in almost every country in the world and in virtually all sectors of the global economy.

The global penetration the internet and (especially) mobile devices has dramatically pushed such activities on the internet, particularly on social media platforms. An acceleration that is having a vast and negative impact for legitimate businesses, governments and consumers, and ultimately society as a whole. However, governments and high-tech companies still lack an in-depth awareness of the whole issue and seem uncertain on how to deploy the appropriate resources and prioritization to combating online counterfeiting.

Already in February 2011 the International Chamber of Commerce estimated that such trade would reach $1.7 trillion by 2015[1] (including digitally pirated music, movies and software, which are not covered by our research). Confirming such trend, a June 2015 study produced by the EU's Observatory on infringements of Intellectual Property (IP) rights focused on counterfeiting in the clothing, footwear and accessories sectors[2]. Here are a few highlights from this study:

- 9.7% of sales lost by the sector due to counterfeiting
- €26.3 billion of revenue lost annually by the sector
- €17 billion of sales lost in related sectors
- 363 000 direct jobs lost
- 518 281 direct and indirect jobs lost

[1] http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/BASCAP-Research/Economic-impact/Global-Impacts-Study/
[2] https://oami.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/research-and-studies/ip_infringement/study2/the_economic_cost_of_IPR_infringement_in_the_clothing_footwear_and_accessories_sector_en.pdf

- €8.1 billion of government revenue lost (social contributions and taxes).

Similarly, a 2014 UK government report[3] underlined that IP crime costs the UK economy about 1.3 billion pounds ($1.8 billion) a year in lost profits and taxes. And even if counterfeit sales are, by definition, difficult to tally, some recent estimates for the total value of fakes sold worldwide each year go as high as $1.8 trillion[4] – including everything from software and medicine to detergent and car parts.

Based on these studies and other available data, the United Nation Office on Drugs and Crime paints an even darker picture, explaining that all too often the link between fake goods and transnational organized crime is overlooked: "Criminal organizations are often involved beyond just producing and moving counterfeit goods, with many also trafficking drugs, firearms and people"[5].

Needless to say, the successful combination of internet and mobile devices has further exacerbated this global problem. Such activities as illicit goods counterfeiting, unauthorized use of trademarks and copying of copyrighted items have strengthen the organized crime and given rise to new kinds of illegal groups/activities. Quickly adapting the traditional techniques of the 'real world', these entities are setting up a variety of online stores that are easily finding a huge audience thanks to e-mail spam, fora, blogs, and, more recently, through a massive use of social network platforms, well-known IM apps and smartphone applications.

[3] http://www.bloomberg.com/news/articles/2016-02-23/cartier-montblanc-win-court-order-blocking-sites-selling-fakes-ikzgc8tw
[4] http://www.economist.com/news/business/21660111-makers-expensive-bags-clothes-and-watches-are-fighting-fakery-courts-battle
[5] https://www.unodc.org/toc/en/crimes/counterfeit-goods.html

2. Fake luxury items proliferating online

Traditionally, the deluge of watches, bags, clothing, jewellery and perfume make up most of the goods seized at borders (see chart).

While smuggling (and money laundering) have always existed, the recent collapse of the Iron Curtain and state deregulation have driven a strong increase in global trade in illegal goods and services. As explained by Moises Naím, renowned expert and author of the 2006 bestseller *Illicit: How Smugglers, Traffickers, and Copycats are Hijacking the Global Economy*, this situation underlines the struggle between traffickers and the hamstrung bureaucracies trying to control them:

> *The diffusion of power to individuals and groups, and away from sovereign states, has created a smuggler's nirvana, in which the lines between legitimate and illegitimate economic activity are blurred and criminal networks possess an unprecedented degree of political influence.*

In other words, along with illegal migrants, drugs, weapons and laundered money, counterfeited goods are part of a global black market whose enormous profits are then reinvested to create new businesses, enable terrorists, and even

to take over governments. While national and international authorities have failed to keep up with this constant growth, the global black market is rapidly moving from the streets to the internet, with counterfeiters becoming more technologically adept, more difficult to track – and harder to pursue in court. In a July 2015 attempt to do just that, the American Apparel & Footwear Association demanded that Alibaba, a large Chinese e-commerce platform, cracked down on thousands of counterfeiters selling expensive bags, clothes and watches, including those of prestigious brands as Hermès, Tiffany, and Gucci[6].

While many products sold (at highly uneven prices) on such websites are genuine, many are not. More pervasive are those posing as legitimate sellers of discounted goods. They also deploy sophisticated strategies: domain names may be registered in one country, servers in another, payment-processing elsewhere and shipping from yet another place. Roxanne Elings, a lawyer at Davis Wright Tremaine, says one counterfeit outfit may run as many as 14,000 websites. Recently other important brands of fashion and luxury items took to court e-commerce giants like Alibaba and eBay[7]. And in late December 2015, Alibaba got a clear message from its direct competitor, JD.com: "Cracking down on fakes is easy. It would take a programmer only a day to do it," said Mr. Liu, CEO of JD.com. "Can you imagine buying a Gucci bag for 80 yuan (US$12.47)?"[8].

Indeed, this global trend has grown exponentially since our previous research, "Online Advertising Techniques for Counterfeit Goods and Illicit Sales"[9], published in November 2014 by Bloomberg and focused on counterfeited clothing sold through Facebook sponsored ads. Among other data, we discovered a lack of security features and transparent policies in most of these online stores. In some cases, their payment system gateways have been set up specifically to accept payments about illicit goods (see image below).

[6] http://www.economist.com/news/business/21660111-makers-expensive-bags-clothes-and-watches-are-fighting-fakery-courts-battle
[7] http://www.reuters.com/article/us-alibaba-lawsuit-fake-idUSKBN0O02E120150518
[8] http://www.wsj.com/articles/jd-com-presses-rival-alibaba-over-fake-goods-1449693181
[9] www.bloomberg.com/news/2014-11-13/fake-out-many-luxury-items-advertised-on-facebook-are-phony-researchers-say.html

Addressing this specific issue, the International Trademark Association[10] used our figures and other data to put pressure on governments, companies and online platforms toward a coordinated effort to curb such illegal activities. However, it is becoming increasing evident that all the stakeholders involved (consumers included) must first reach a better understanding of this online global threat. Even beside the actual sale trade, we should pay close attention to creative selling practices, how and where items are offered, what techniques are deployed to avoid authorities, and innovative ways to reach potential customers. – as detailed in an excellent overview published by Bloomberg last summer ("Luxury Firms Fight Online Fraudsters Over Expensive Fakes")[11].

[10] http://www.inta.org/Press/Pages/2014Holidays.aspx
[11] http://www.bloomberg.com/news/articles/2015-07-27/fakes-at-7-800-send-luxury-companies-online-to-fight-fraudsters

3. Global counter-strategies…going nowhere?

To be fair, in recent months we witnessed an increased collaboration among internet stakeholders and authorities worldwide – along with a renewed commitment toward a unified effort to curb the online illicit trade. For instance, even if China is widely considered the top producer of counterfeit items, the Chinese government alerted its citizen about online purchases and related dangers[12].

Last year, WeChat (a mobile text and voice messaging communication service developed by Chinese company Tencent in 2011), has also blocked about 7,000 accounts selling fake goods, followed by a broader coverage on China Daily: "WeChat launched a trademark protection mechanism last year, which involves about 40 trademark right owners that have more than 100 brands, including well-known international brands such as Louis Vuitton and Chanel.[13]"

The UK and Chinese governments signed an agreement about joint monitoring strategies addressing online sales[14], while in the US the FBI is working with the DoJ to aggressively look up for counterfeit items available on major e-commerce platforms[15]. And last June over 4,300 posts and 20 profiles promoting illegal sales were deleted on Facebook after an extensive UK police operation[16].

To further understand the wider ramifications of such phenomenon, it is useful to take a look at Google's latest report about online advertising: "Google disabled 49% more ads in 2015 than the prior year, as the Internet giant developed new ways to detect a rising tide of dubious online marketing tactics. … it removed more than 780 million ads in 2015 for violating its policies, up from 524 million in 2014, 350 million in 2013 and 220 million in 2012"[17].

Hinting at another major issue in this context, Tom Siegel, vice president of Google's Trust & Safety group, added: "In 2016, Google said it would work to crack down on fraudulent clicks by automated computers known as bots. The bots can be costly to advertisers, who pay Google each time a user clicks on their ad". As detailed in our research

[12] http://www.theguardian.com/world/2015/nov/03/china-warns-its-citizens-things-you-buy-online-might-be-fake
[13] http://www.chinadaily.com.cn/cndy/2016-01/20/content_23157959.htm
[14]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/500740/China_IP_Newsletter__February_2016_.pdf
[15] http://www.theverge.com/2015/10/5/9452939/fbi-counterfeit-goods-department-of-justice
[16] http://www.independent.co.uk/life-style/gadgets-and-tech/news/police-deleting-thousands-of-facebook-posts-in-operation-jasper-privacy-crackdown-10345388.html
[17] http://blogs.wsj.com/digits/2016/01/21/google-disabled-49-more-ads-in-2015/

and here below, bots are indeed a huge threat for the online ecosystem and widely used to promote illicit online trafficking.

But despite this increasing effort at global level, particularly in Western countries, a December 2015 poll revealed that "millions of online shoppers are being duped into buying counterfeit products with one in four being ripped-off"[18].

In other words, a pivotal report produced in 2009 by Moises Naím ("Five Wars of Globalization") is more relevant than ever and his suggestions are still pending: "Like the war on terrorism, the fight to control these illicit markets pits governments against agile, stateless, and resourceful networks empowered by globalization. Governments will continue to lose these wars until they adopt new strategies to deal with a larger, unprecedented struggle that now shapes the world as much as confrontations between nation-states once did"[19].

4. Bots and AI as tools for online illicit trade

Our June 2015 research ("Instagram spam-bots and social media popularity") explained that the popular social network is actually infested with millions of spam-bots and fake accounts[20] – despite boasting 400 million users in September 2015[21]. The subsequent "internal cleansing" however, did little to curtain a tendency that is instead spreading to other social platforms. According to a March 2016 story on the *New York Times*, it could be plausible that "Instagram May Change Your Feed, Personalizing It With an Algorithm"[22]. The truth is that bots and algorithms are responsible for so many activities on today's internet and we are facing an emergent kind of bot, capable of autonomous interaction with humans and even acting on their behalf.

In detailing such progress, a recent story on VICE[23] explains that "excitement about bots, from Silicon Valley to the academy, is palpable at the moment [and] …we must consider, however, the fact that this technology will continue

[18] http://www.mirror.co.uk/news/uk-news/quarter-shoppers-been-duped-buying-6950299
[19] http://foreignpolicy.com/2009/11/03/five-wars-of-globalization/
[20] https://www.scribd.com/doc/270100229/Instagram-Research-June-2015
[21] http://blog.instagram.com/post/129662501137/150922-400million
[22] http://www.nytimes.com/2016/03/16/technology/instagram-feed.html?ref=technology&_r=0
[23] http://motherboard.vice.com/read/how-to-think-about-bots

to evolve and become more sophisticated." Microsoft has launched a new division focused on chatbots (with an exclusive report on Bloomberg[24]), while Google is working on a similar project since last June: according to BusinessInsider[25], "researchers said they found it encouraging that the model can remember facts, understand contexts, perform common-sense reasoning without the complexity in traditional pipelines."

As a result of this general trend, bots, algorithms and AI software are also being deployed to advance counterfeit trade among social media users. Indeed, our own research revealed that an army of bots is busy promoting fake items online. More often than not, they provide several important benefits in regards to human operators, including:

- Automate their publishing process and activities;
- Monitor and follow social media users that searched or posted content with specific hashtags (ie, #handbag, #LouisVuitton);
- Publish simultaneously from multiple accounts in order to "flood" hashtags or topics related to fashion brands, thus always attracting new customers;
- Ability to use IP proxy to mask their identity and thus meddling with law enforcement activities;
- Less expensive than humans and being active 24/7;
- Great for info gathering and data mining.

That said, the bots we met in our Instagram research featured limited capabilities and most of them were unable to interact properly and keep a conversation with sensible answers. However, their general level of automation seems good enough for their main function: promoting an illegal business and encouraging to buy fake items. In fact, a 2014 story on *Venture Beat* was already exposing these trafficking activities related to fashion brand items on Instagram[26].

[24] http://www.bloomberg.com/features/2016-microsoft-future-ai-chatbots/
[25] http://uk.businessinsider.com/google-tests-new-artificial-intelligence-chatbot-2015-6?r=US&IR=T

[26] http://venturebeat.com/2014/08/21/instagrams-brand-problem-the-fakes/

5. In search of ‘legitimate’ sellers of counterfeit goods

Our research project started by detecting and identifying sellers of counterfeit goods on Instagram. By focusing on certain account features, we developed an algorithm able to identify several active botnets. Here is a short list of such features and their importance level:

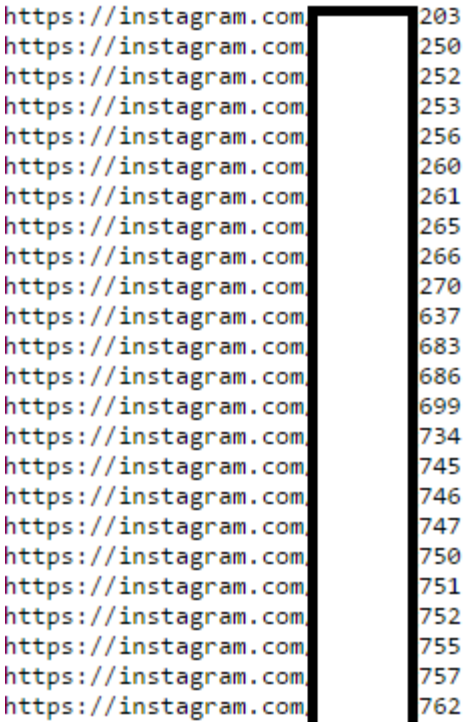
General features	Bot features
Nickname	Nickname
	Name and surname
profile description	profile description
web site	web site
post details and hashtag	post details and hashtag
last 20 posts	last 20 posts
	post frequency
	Ratio following/followers

Importance
Low
Medium
High

A quick look at those user nicknames reveals that they are just bots part of a wider botnet. The following ones include random characters but are all of the same length:

https://instagram.com/ugnr
https://instagram.com/qpit
https://instagram.com/uhvo
https://instagram.com/twwh
https://instagram.com/pmzq
https://instagram.com/mxvk
https://instagram.com/axpd
https://instagram.com/pcoz
https://instagram.com/lrra
https://instagram.com/tunk

Others include a mix of common characters with sequential or random numbers:



Other key features are the same words used in each user/bot bio and contact info (email, phone #, IM), along with the same terms related to counterfeit market (“cheap”, “replica”, original”, etc.) or to targeted brands (handbags, LV, shoes, etc.).

When dealing with botnets, a reference website has less relevance in itself (most just use shorting URL services such as Google and bit.ly or simply do not have a home website), while post descriptions and hashtags are key features to reveal an illicit website. Indeed, the most recent 20 post of a given website include same keywords, hashtags, and contact info just mentioned.

Some bots publish more than one post hourly for the entire day, but we cannot rule out that some accounts are managed by several people in order to be active 24/7.

In general, the following/followers ratio is a relatively trivial feature, even if some of them follow large crowds, also because many bots follow each other in order to lower this ratio.

Also, after verifying manually each bot account collected through our algorithm, we discovered that some legitimate accounts were also included. Therefore, we refined our algorithm and excluded those accounts whose profile description or posts included the following terms:

Keyword Profile	Keyword Post
am	am
pm	pm
a.m	a.m
p.m	p.m
Street	Street
Avenue	Avenue
ZIP	ZIP
Square	Square
Plaza	Plaza
Personal Shopper	Personal shopper
Personal Buyer	Personal buyer

Those accounts we identified as bots are often generated by some software, while just a few others are created by an actual person. Features like nickname, picture quality, and profile description are key to understand how they were created. This does not necessarily mean that an account generated by a software is also managed by a software instead of a person, and vice versa. As mentioned above, it could be that some accounts are generated by a software, but then maintained by various people.

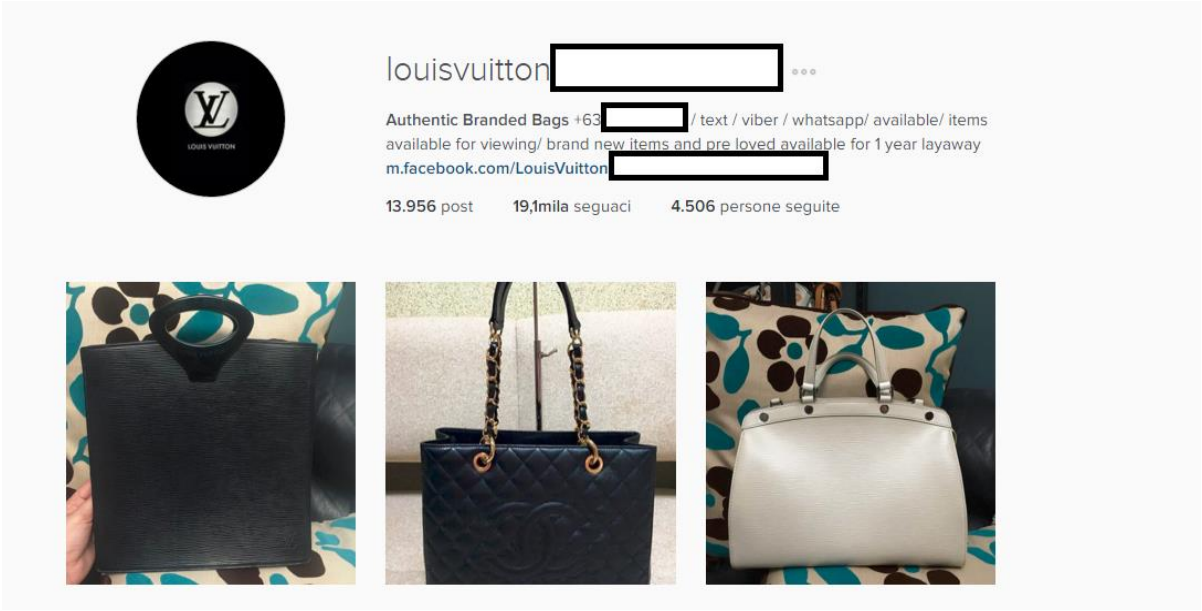
Account generated by
Human
Bot

Name+Surname
Surname+Name
Name+Surname+Random numbers
Surname+Name+Random numbers
Random numbers+Name+Surname
Random numbers+Surname+Name
Adjective+Key word
Adjective+Key word+Random numbers
Key word+Brand Name
Random chars

6. Key stats and features of fake accounts

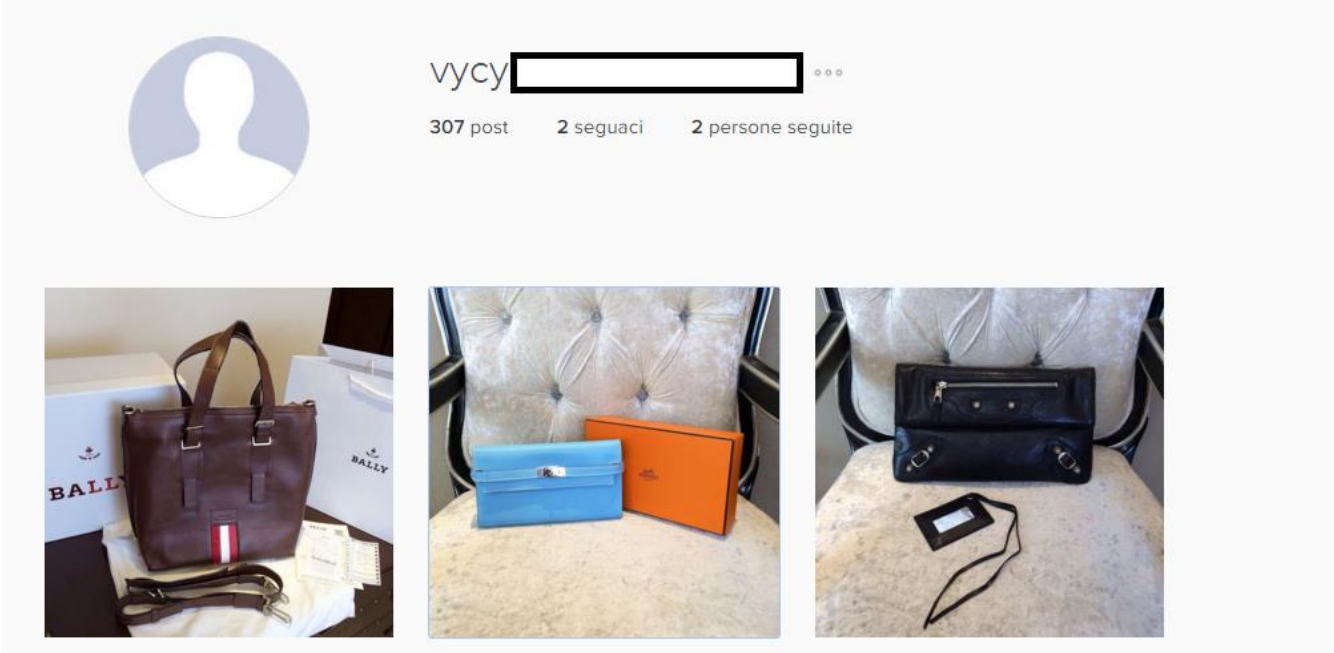
We identified a variety of Instagram spam-bots: some sported a good quality, in order to resemble legitimate vendors, while others were clearly created only for spamming at will. Here are a few examples.

The following user-bot published almost 14,000 post and has 19,000 followers, showing a certain attention to detail in order to look legitimate:



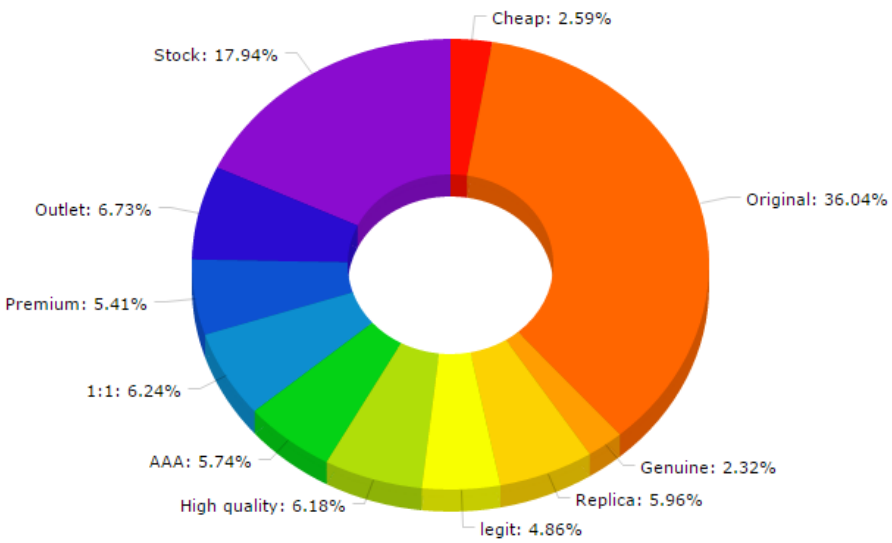
The following Instagram account, also seemingly part of the Louis Vuitton group, sells counterfeit luxury items of different brands, including the Chanel bag pictured below. This specific account seems based in China.

Finally, the following pictures are typical of a good quality bot profile (the second one clearly China-based) whose only purpose is to spam at large.



7. Profile keywords and posting techniques

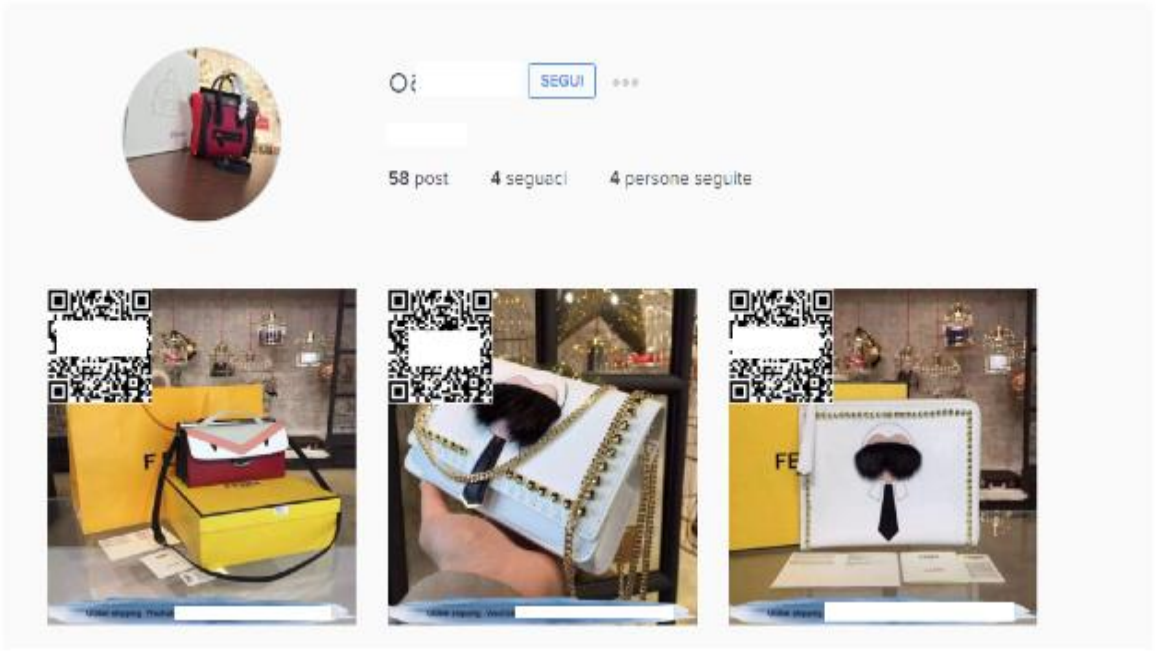
As mentioned above, most Instagram accounts selling counterfeit items share several keywords. While “original” is by far the top term (36,4%), the combination of other keywords such as “Replica”, “AAA” and “1:1” (used to describe a fake item but very similar to the original) cover about 18% of total terms. These profile keywords (detailed in the following pie chart) helped us to correctly identifying the fake accounts selling counterfeit items (20,892 that posted a total of 14.5M posts).



In order to unveil such structured and ramified activities, we spent a lot of time in studying each post wording and frequency, along with their specific hashtags and images. Many sellers feature a "classical" outline (as depicted below): a generic image with a short description, detailed contact info and several hashtags of famous brands to attract a broader audience.

However, most likely the Instagram algorithm “police” is on constant alert about fake/suspicious accounts using common hashtags or keywords or external contact info (ie, WeChat), and was able to identify and remove many of them. To get around this detection process, some sellers are publishing only images embedded with their contact details, as shown below.

As a variation of this work-around, some sellers incorporate a QR code in the same item image, while others include their contact details in their own profile (here below, respectively):


SEGUI
58 post
4 seguaci
4 persone seguite


Piace a riserelp,
_4_the_love_of_fashion_,
billionairentourage, zapoljva_lolita,
billionaireave, deryamavi77,
iamkingfloyd, uberluxe,
finesmycoinzfree e
her TopCHANEL reel
imports Australian wild boa constrictors
ablaze photo images, with imported texture
within [good] [good] thick soft delicate
collocation pearl gold hardware - size 25
a1022800 luxury atmosphere
Top#chanel#chanellover#chanelbag

8. IM apps as top communication tools

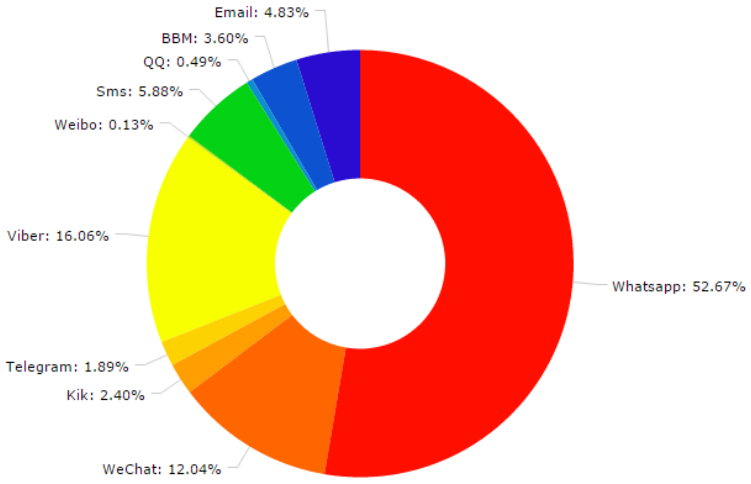
Until a few years back, this peculiar e-trade took place mostly on dedicated websites, often disguised within the so-called "deep web". Today, however, most counterfeit item sellers shifted to common IM apps or chat rooms – faster, effective and widespread tools enabling transactions across the world.

Indeed, managing these activities though a website results in several problems, including:

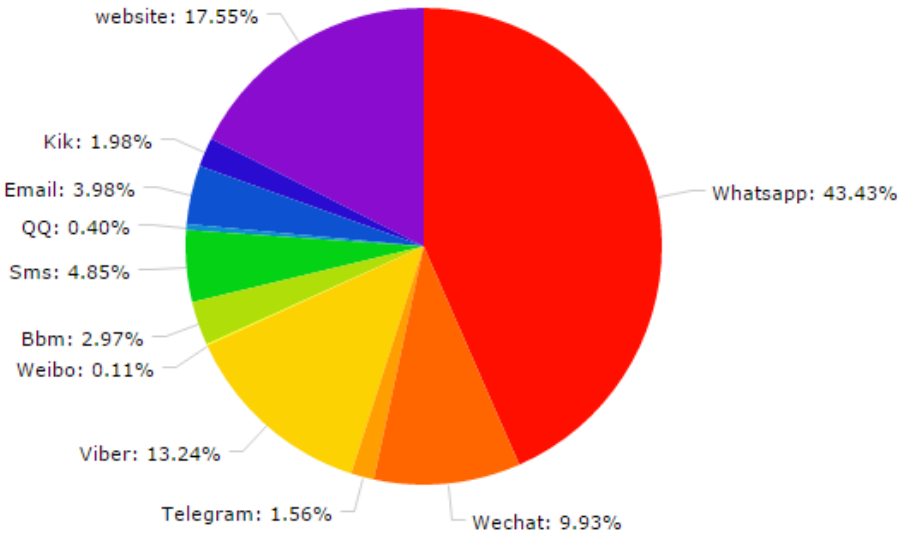
- On-going investments in money and human resources for set-up, registration, hosting, maintenance and so forth.
- Security concerns due to personal data needed for domain registration and payments (fake data won't work for credit card transactions).
- In case of website closure or seizure (a frequent occurrence in this trade), the entire process must be activated again and again.

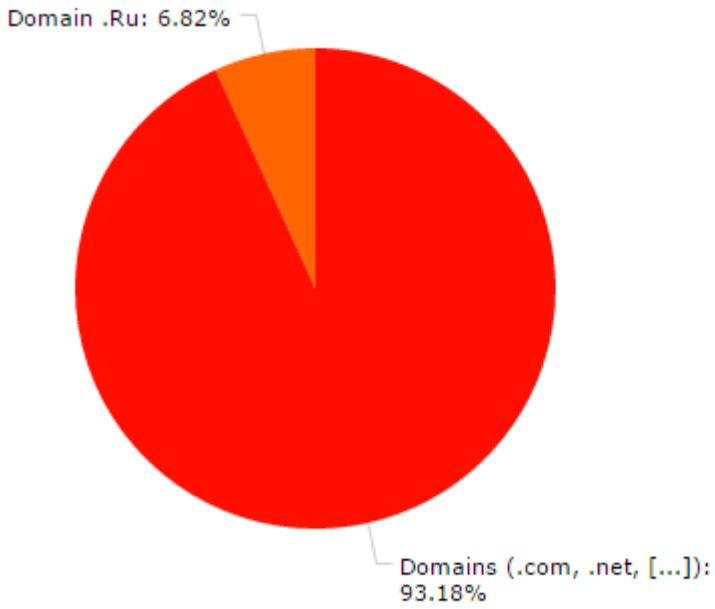
Current IM apps are an effective solution to these issues, while ensuring at the same time a protective layer: popular apps such as Telegram and Whatsapp both provide end-to-end encryption. Generally speaking, these services are not actively pursuing these sellers and only recently WeChat managers noticed that their service is being mostly used for counterfeit sales, while still struggling to come up with an effective counter-strategy. Indeed, account closure is a very rare event since it requires a detailed proof of ToU misuse or abuse. In case, opening a new account is just a few clicks away. And needless to say, IM apps provide easy interaction and multimedia options – enough to satisfy any kind of consumer.

Our study revealed that over 75 per cent of seller accounts enlist two contact methods, with a strong preference for Whatsapp and a growing share for WeChat – as shown in the following pie chart:

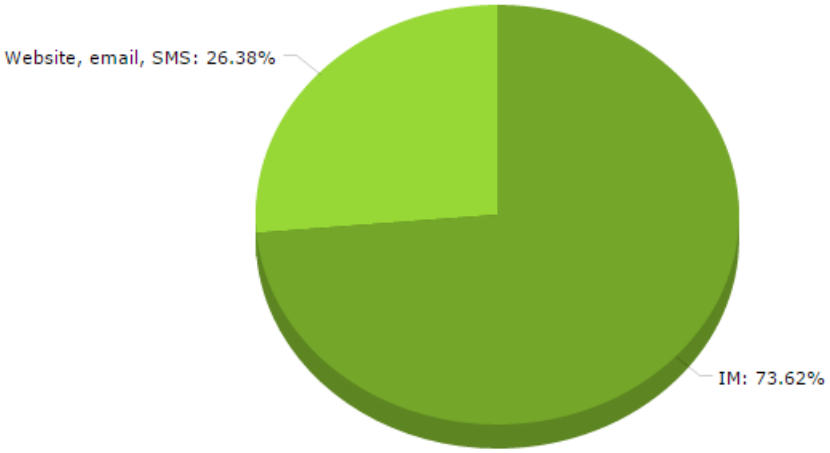


Taking also into account the incidence of websites, we have a slightly different outline: they cover about 17 per cent of total market and almost 7 per cent have a Russia-based domain (.ru) – as shown in the two charts below:



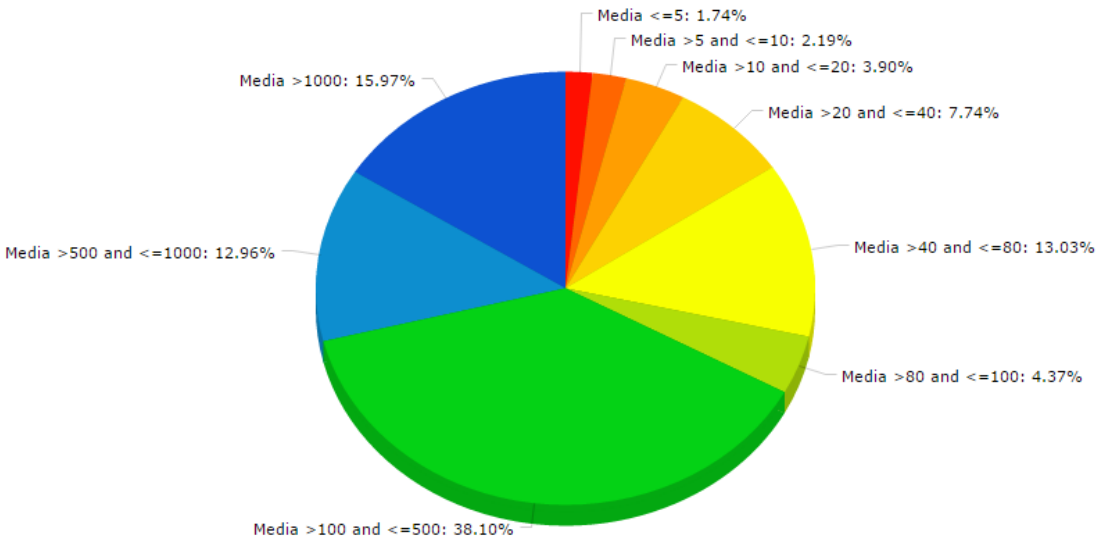


Finally, the following comparison chart between “old fashioned” tools – email, websites and SMS – and new IM apps explains the communication shift currently taking place in the overall counterfeit market:


Website, email, SMS: 26.38%
IM: 73.62%

9. Instagram spam-bot activities

As mentioned earlier, we also monitored the following/followers ratio and posting activities of those Instagram accounts (20,892) selling counterfeit items (including both spam-bots and human-managed accounts).



As shown in the previous chart, 38 per cent of those accounts posted between 100 and 500 images, while almost 13 per cent posted less than 1,000 pictures. These overall figures reflect an intense posting activity – especially if compared to the results of our June 2015 study, where an actual Instagram user posted an average of 55 images against 6 images posted by a bot. A wide difference obviously due to the fact that this posting activity is specifically aimed at advertising the sale of fake luxury items.

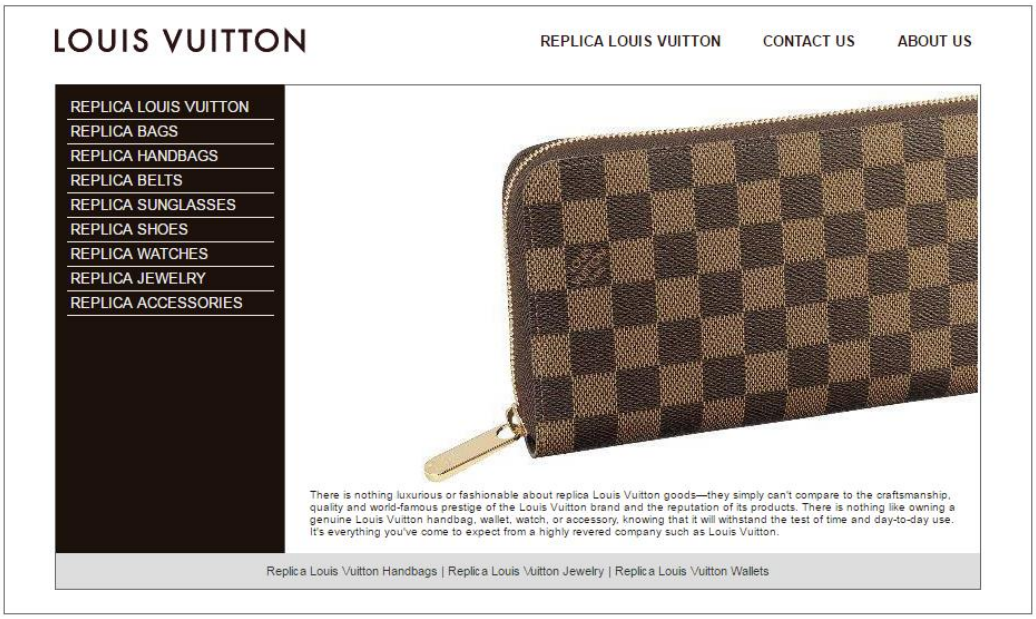
Also, more than 40 per cent of these Instagram accounts features over 1,000 followers each, with an additional 11 per cent that have between 500 and 1,000 followers. Overall we face quite relevant figures: obviously these accounts strive to appear legitimate and to attract many real followers (beside a small percentage of bots). In other

words, as mentioned in the same 2014 *Venture Beat* story[27], these fake Instagram accounts were successful in deceiving people by purportedly showing to be part of a famous brand network.

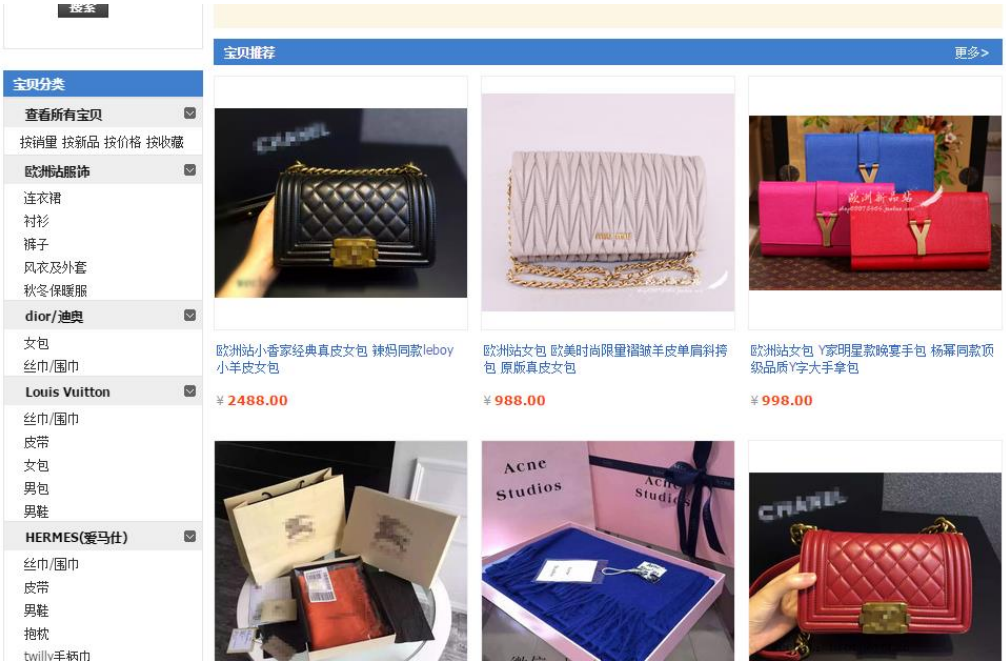
10.Fraud and counterfeit activities on the web

Even with a lower impact than a few years ago, there is no lack of fraudulent websites out there. A closer look at this share provides an outcome similar to that of our previous research on sponsored Facebook ads[28]. First of all, most websites are de facto anonymous: they take advantage of the Whois privacy protection in order to hide data about the domain owner, address, etc. Many are in fact large portals featuring a great variety of items and luxury products. Others try hard to copy the original design of famous brand websites, thus attempting to pass as legitimate e-commerce sites. Some are quick to brand themselves as "outlet" store or use ambiguous terminology in order to justify the ridiculous price of their "original" merchandise. In the following screenshot, a fake Louis Vuitton website puts in the foreground the word "replica" for every item:

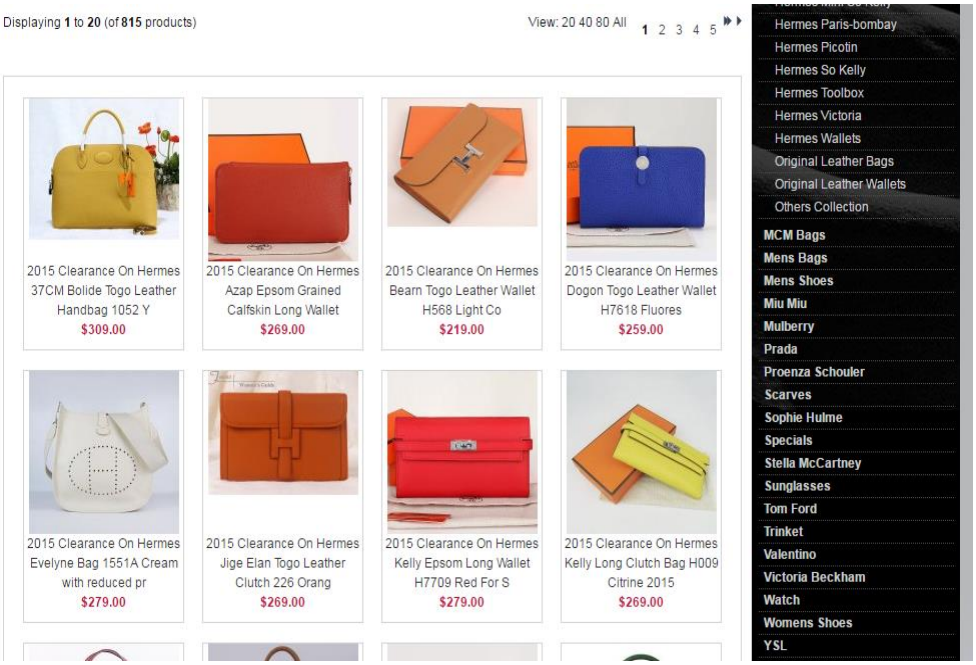
[27] http://venturebeat.com/2014/08/21/instagrams-brand-problem-the-fakes/
[28] http://nymag.com/thecut/2014/11/facebook-is-littered-with-ads-for-luxury-fakes.html



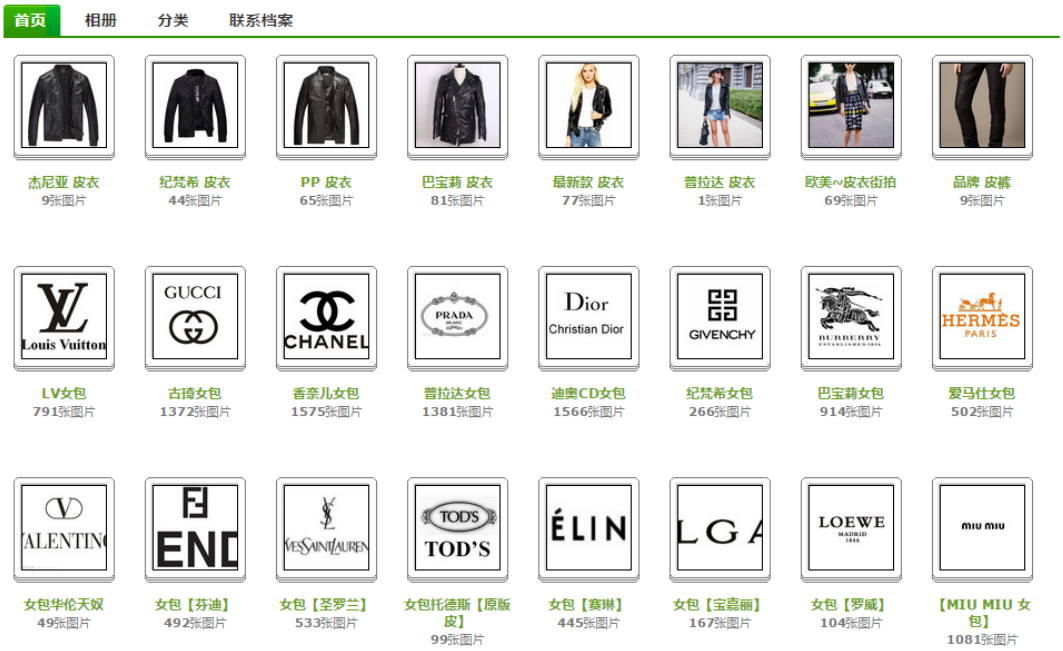
In another example, a Chinese website provide a wide range of products divided by categories and brands:

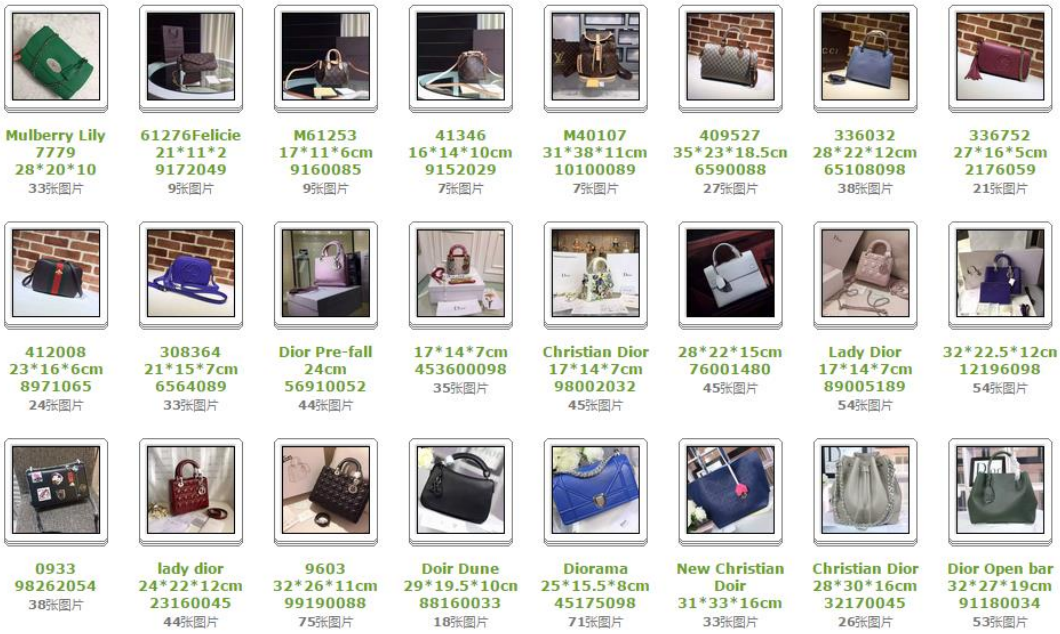


The following website seems a large e-commerce entity, featuring 815 products of the “Hermes” brand (see top left corner) plus a broader selection of other renowned “collections” at reasonable prices

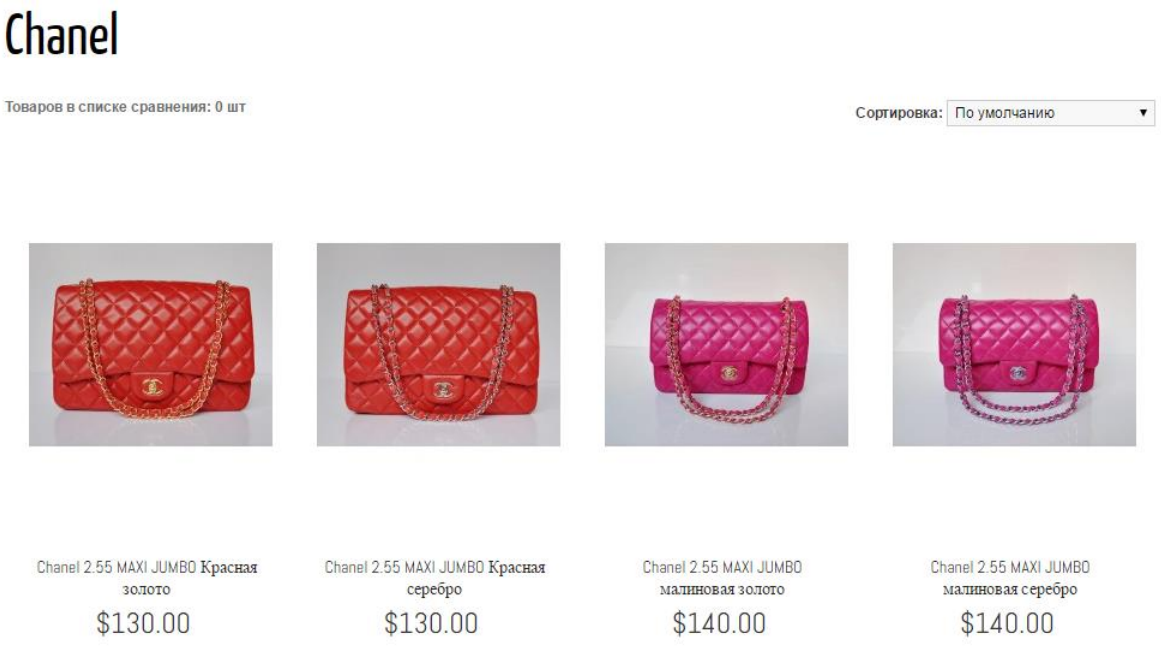


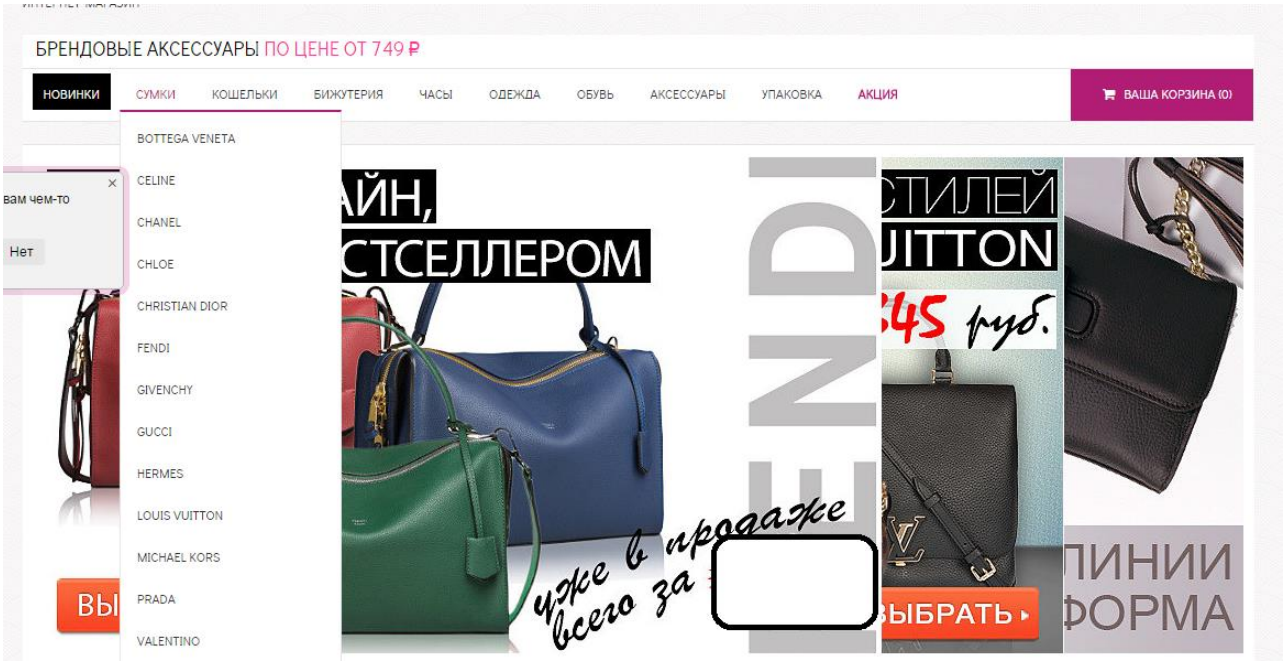
The following screenshots come from Chinese websites: the first one is a photo catalog hosted by Yupoo, part of Alibaba's AliExpress, as is the second one that has many different products for sale.





Finally, here are two Russia-based websites specialized in Chanel bags – again, at quite cheap prices:

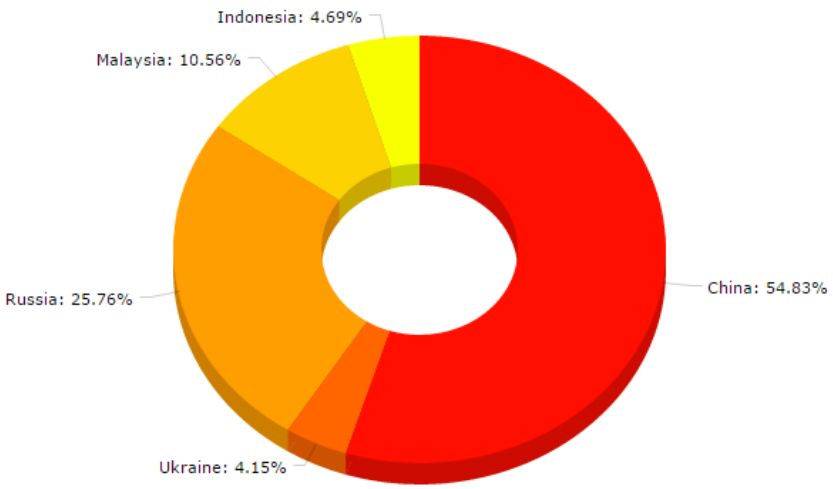



БРЕНДОВЫЕ АКСЕССУАРЫ ПО ЦЕНЕ ОТ 749 ₽
НОВИНКИ
СУМКИ
КОШЕЛЬКИ
БИЖУТЕРИЯ
ЧАСЫ
ОДЕЖДА
ОБУВЬ
АКСЕССУАРЫ
УПАКОВКА
АКЦИЯ
ВАША КОРЗИНА (0)
BOTTEGA VENETA
CELINE
CHANEL
CHLOE
CHRISTIAN DIOR
FENDI
GIVENCHY
GUCCI
HERMES
LOUIS VUITTON
MICHAEL KORS
PRADA
VALENTINO
Нет
СТСЕЛЛЕРОМ
ЫБРАТЬ
ФОРМА

11.Top countries involved

To pin down the countries from where these websites operate we took into account several data: their web domains, phone numbers and email hosting services, along with languages and character coding. These evidences leave little doubts about certain countries, even if we can never have a definitive proof.

The following chart details the top five countries involved in online sales of counterfeit items.

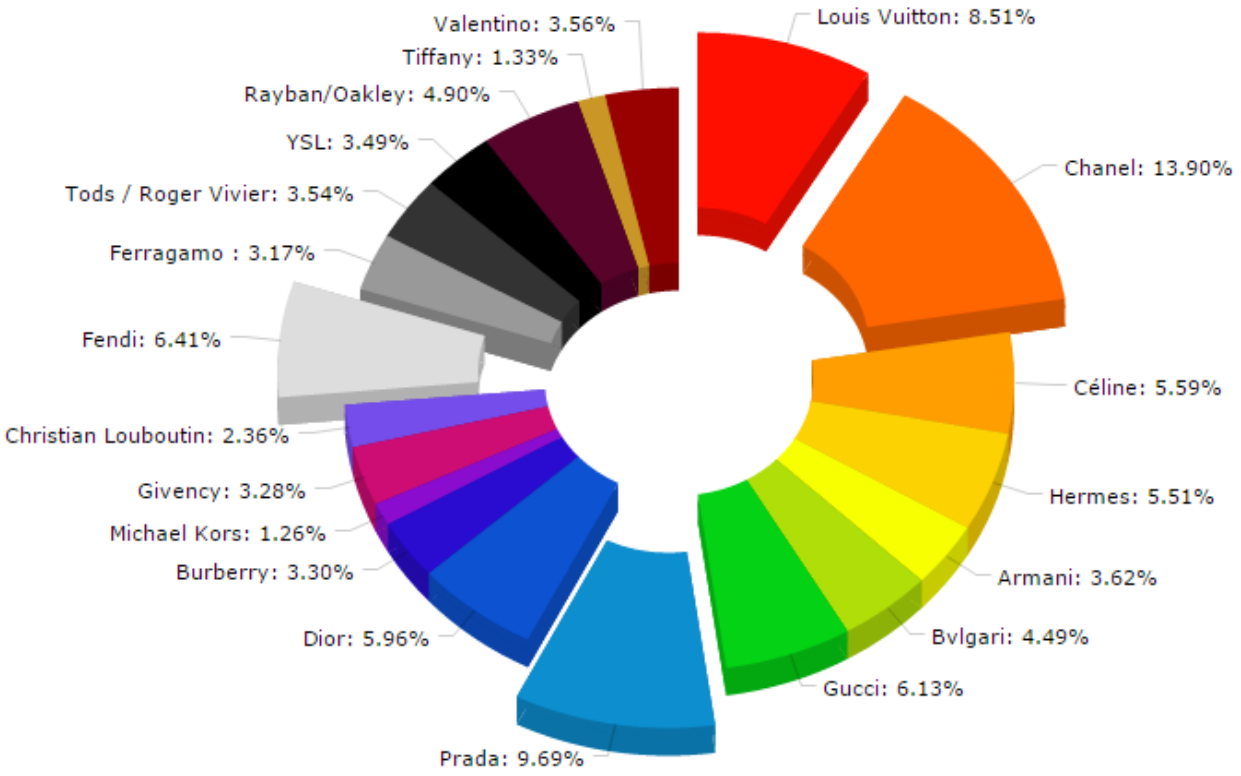


These data are almost identical to those produced by the Office of the United States Trade Representative (USTR). In its 2015 "Special Report 301", four out of these five countries are included in the "Priority Watch List: they "present the most significant concerns this year regarding insufficient IPR protection or enforcement or actions that otherwise limited market access for persons relying on intellectual property protection."

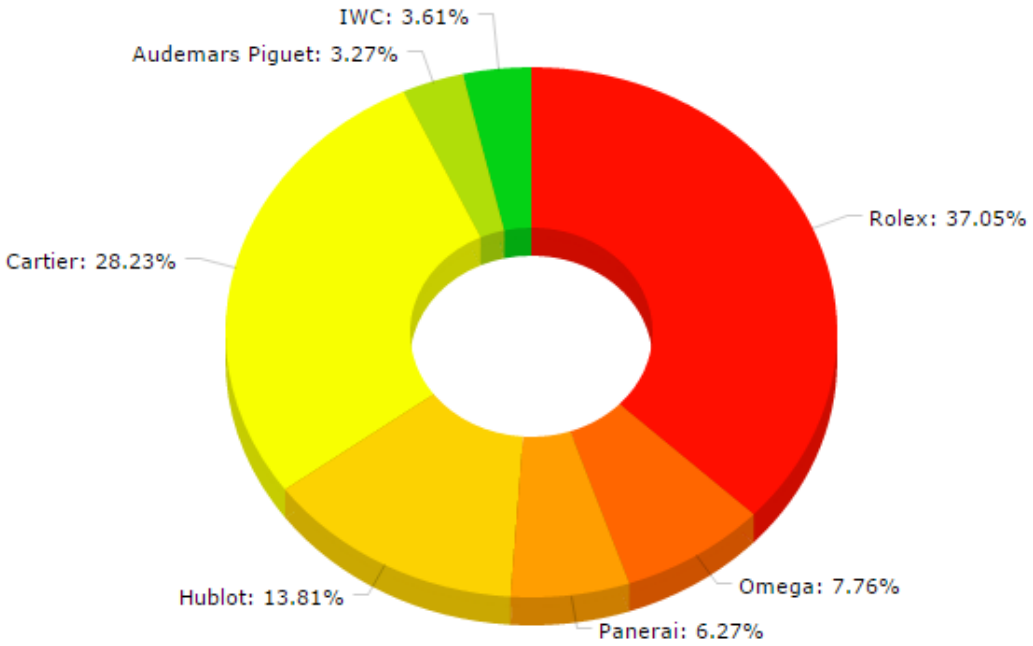
SECTION II. COUNTRY REPORTS 32
PRIORITY WATCH LIST 32
East Asia and Pacific 32
China
Indonesia
Thailand
South and Central Asia 45
India
Pakistan
Near East, including North Africa 53
Algeria
Kuwait
Europe and Eurasia 54
Russia
Ukraine

12.Top counterfeit brands

We took into account over 20,000 images uploaded by those Instagram accounts identified as sellers of counterfeit items. Often such images featured hashtags that did not match their image content and in several cases they included hashtags of different brands, even if they had nothing to do with the items depicted. This is a basic technique to attract a broader audience. After a rigorous analysis, we put together an overview of the brand hashtags more frequently used, including those with a direct correlation with the image content. As detailed in the following chart, the top targeted brands are Chanel, Prada, Louis Vuitton and Fendi.



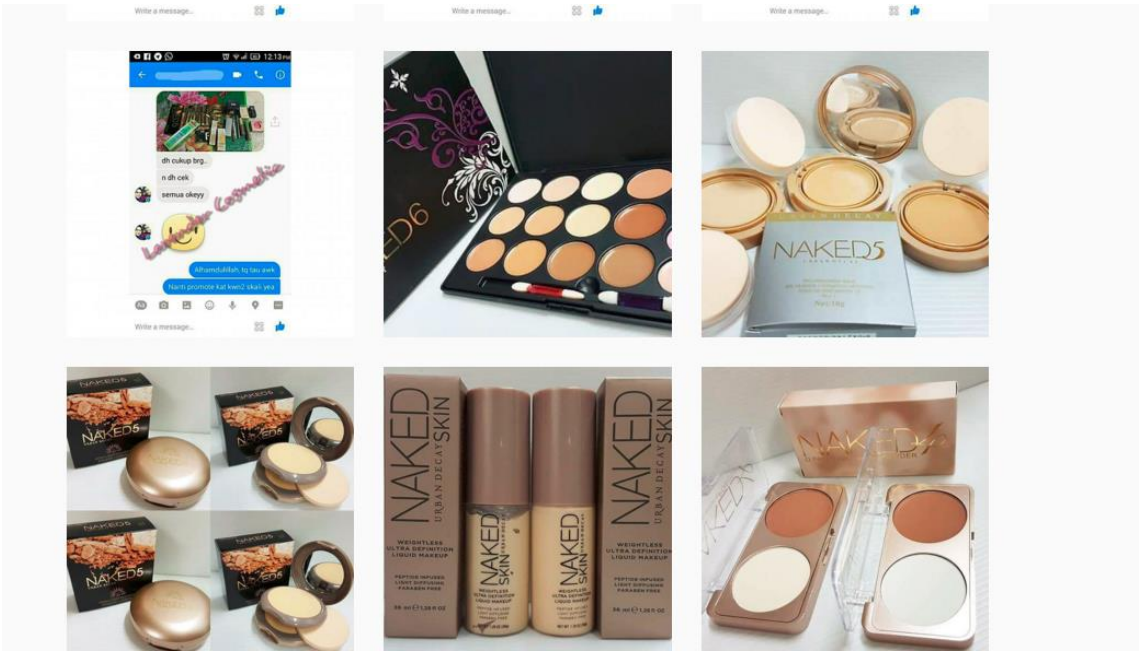
We also decided to take a closer look at fake luxury watches sold via Instagram: Rolex (37%) and Cartier (28%) are still the most sought after, as described in the following chart:



13.Illicit account activities

We monitored the Instagram accounts identified as sellers of counterfeit items (20,892) for three full days, from Friday March 18 to Sunday March 20, 2016. In their overall activities, they gained 687,817 new followers and uploaded 146,958 new images. It's worth noticing, however, that some accounts actually featured less images after those three days. Most probably, they sold out certain items and immediately deleted their images so to avoid useless requests. Another reason to slow down their social media activity could be an attempt to hide blatantly illegal ads.

Browsing through their profiles, we noticed that an Instagram account selling cosmetics and beauty products (shown below) deleted a whopping

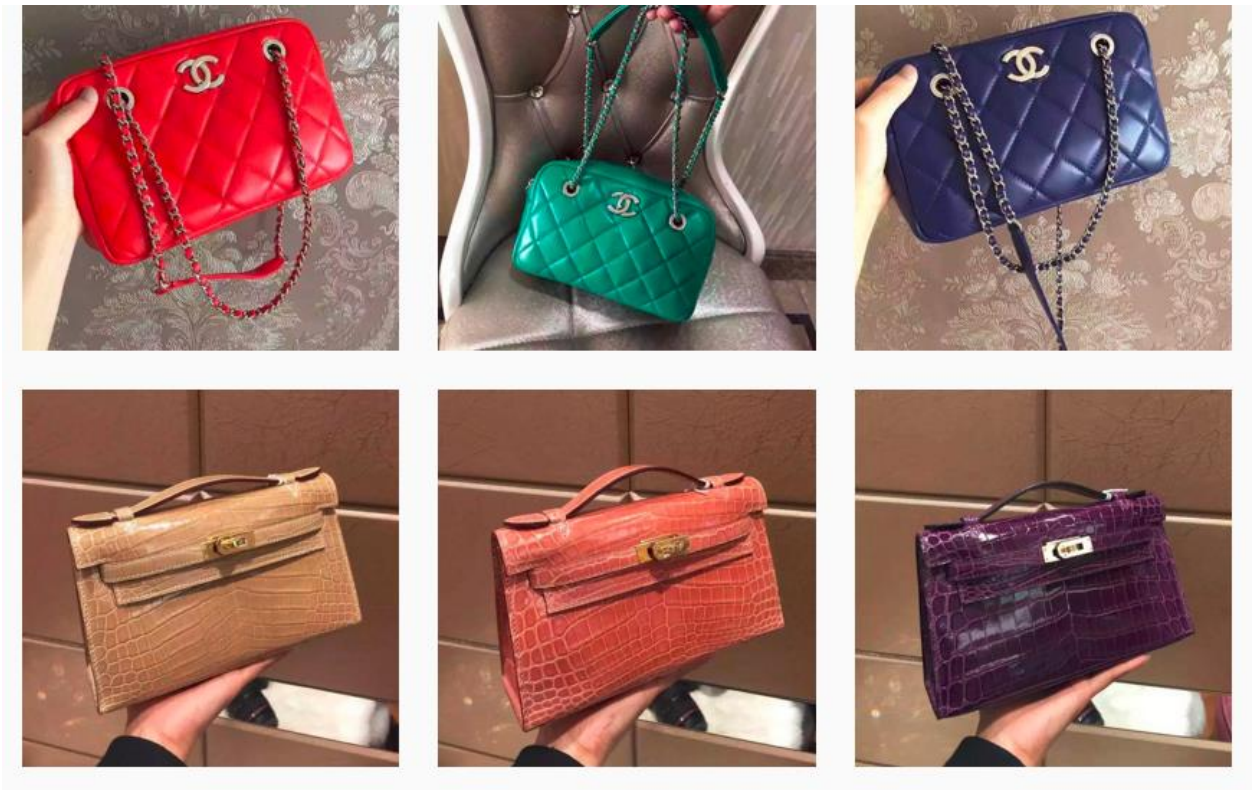


Along those three days, this account deleted a whopping 1,582 images. In addition to the above mentioned reasons, we should keep in mind that cosmetics and beauty products have come under increased scrutiny for their possible effects on human health and on the environment[29]. Therefore, authorities are paying an increased attention to fake or counterfeit items sold directly online.

On the other hand, a China-based seller uploaded about 380 new images in the same three days:

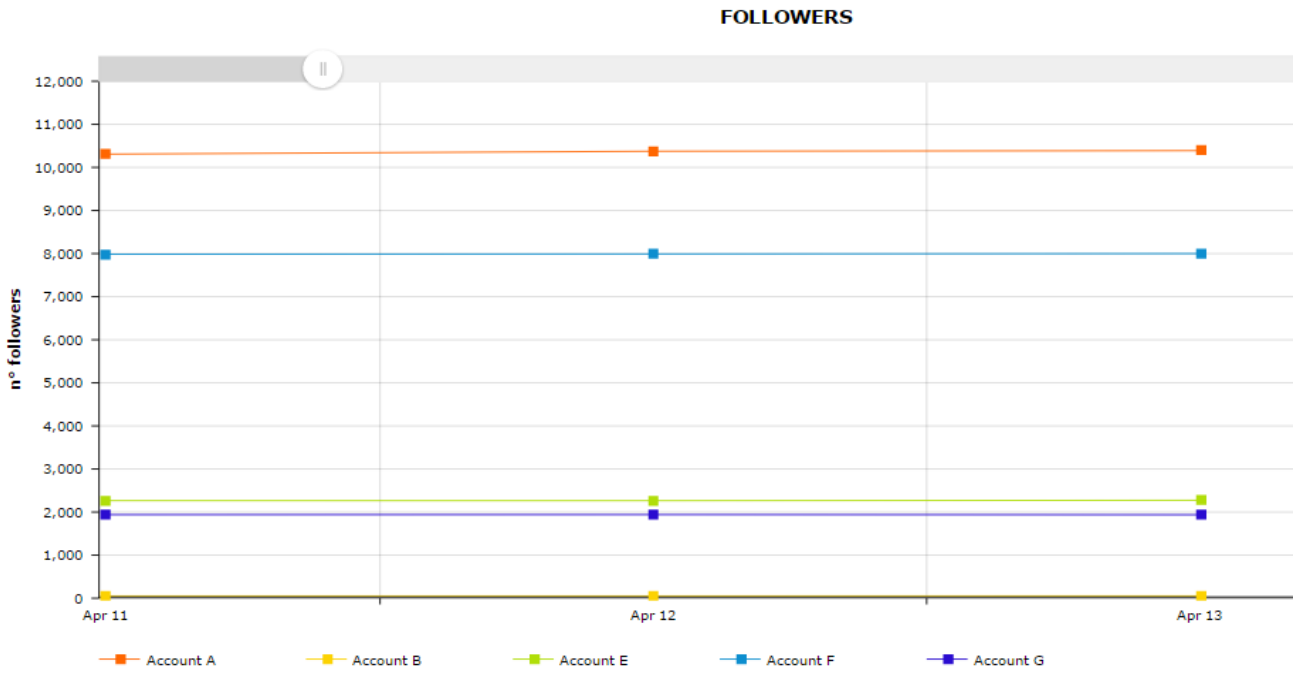
[29] http://www.cancer.org/cancer/cancercauses/othercarcinogens/athome/cosmetics

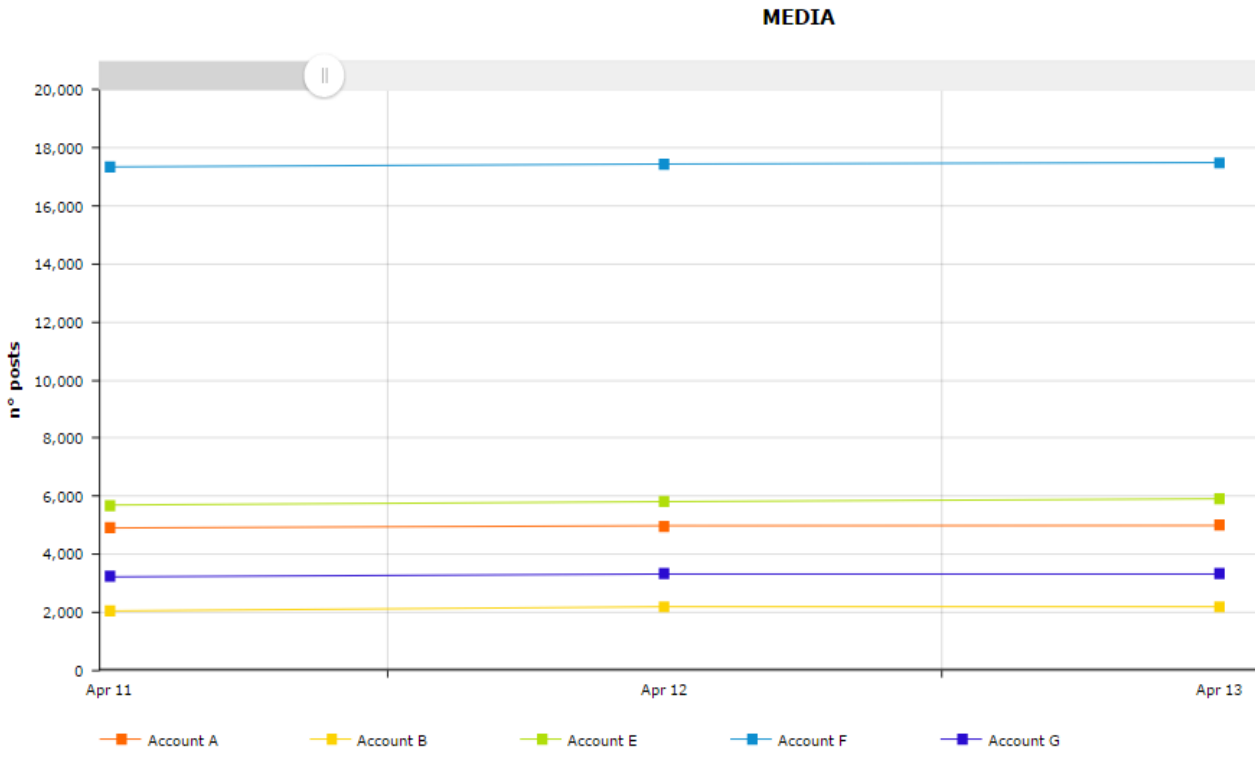
The following accounts, specialized in sales of fake Chanel bags, were able to gain 11,345 and 10,228 new followers, respectively:



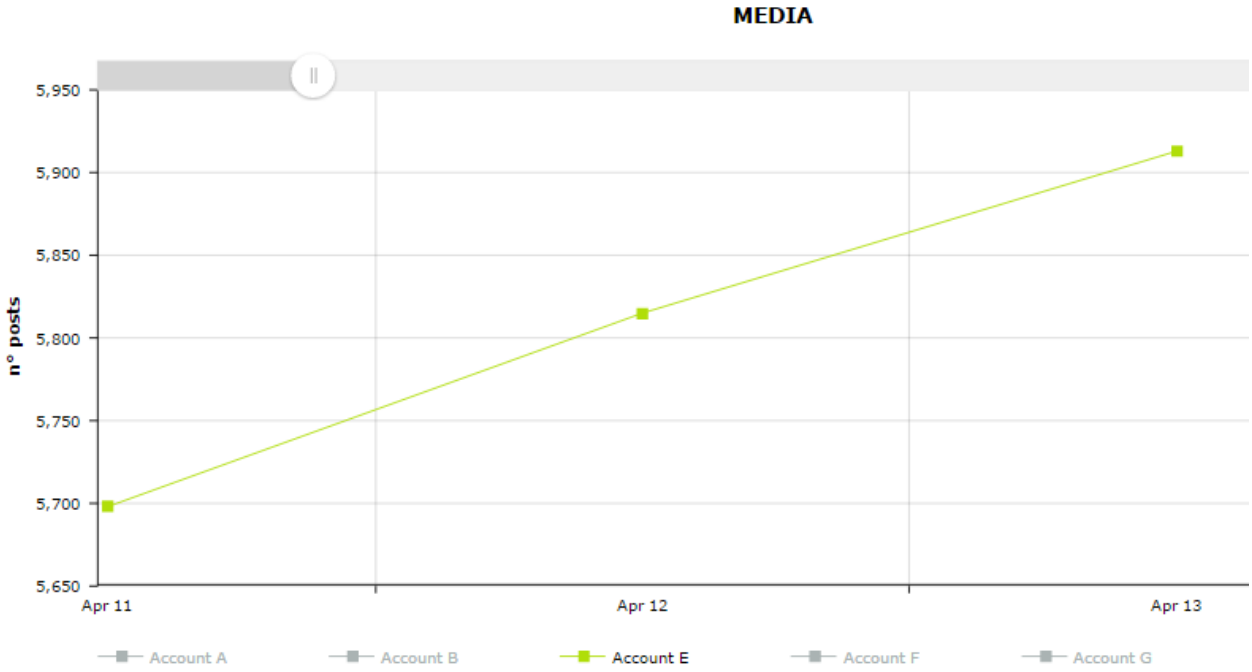
We monitored again the same Instagram accounts for three more days, from Monday April 11 to Wednesday April 13, 2016. Their overall activities recorded 327,076 new followers and 67,566 new images.

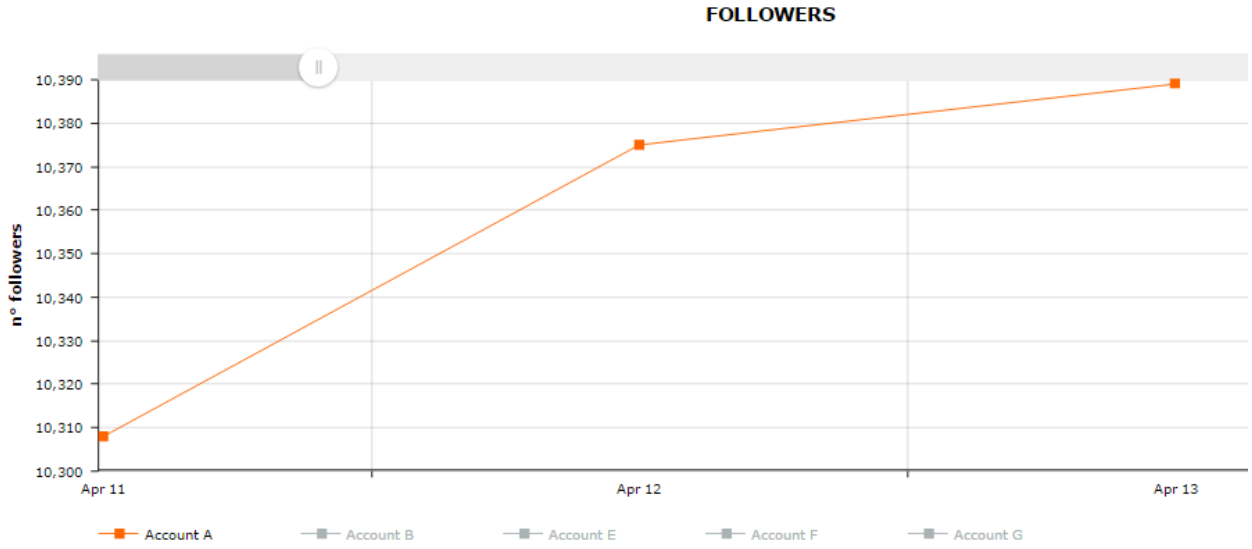
In particular, we studied the activities of five accounts chosen at random, producing the following charts about, respectively, new followers gained and new posts uploaded.





We also extracted specific data related to two individual accounts: new posts for Account E and new followers for Account A, respectively:





Finally, here is a summary of our three-days research studies:

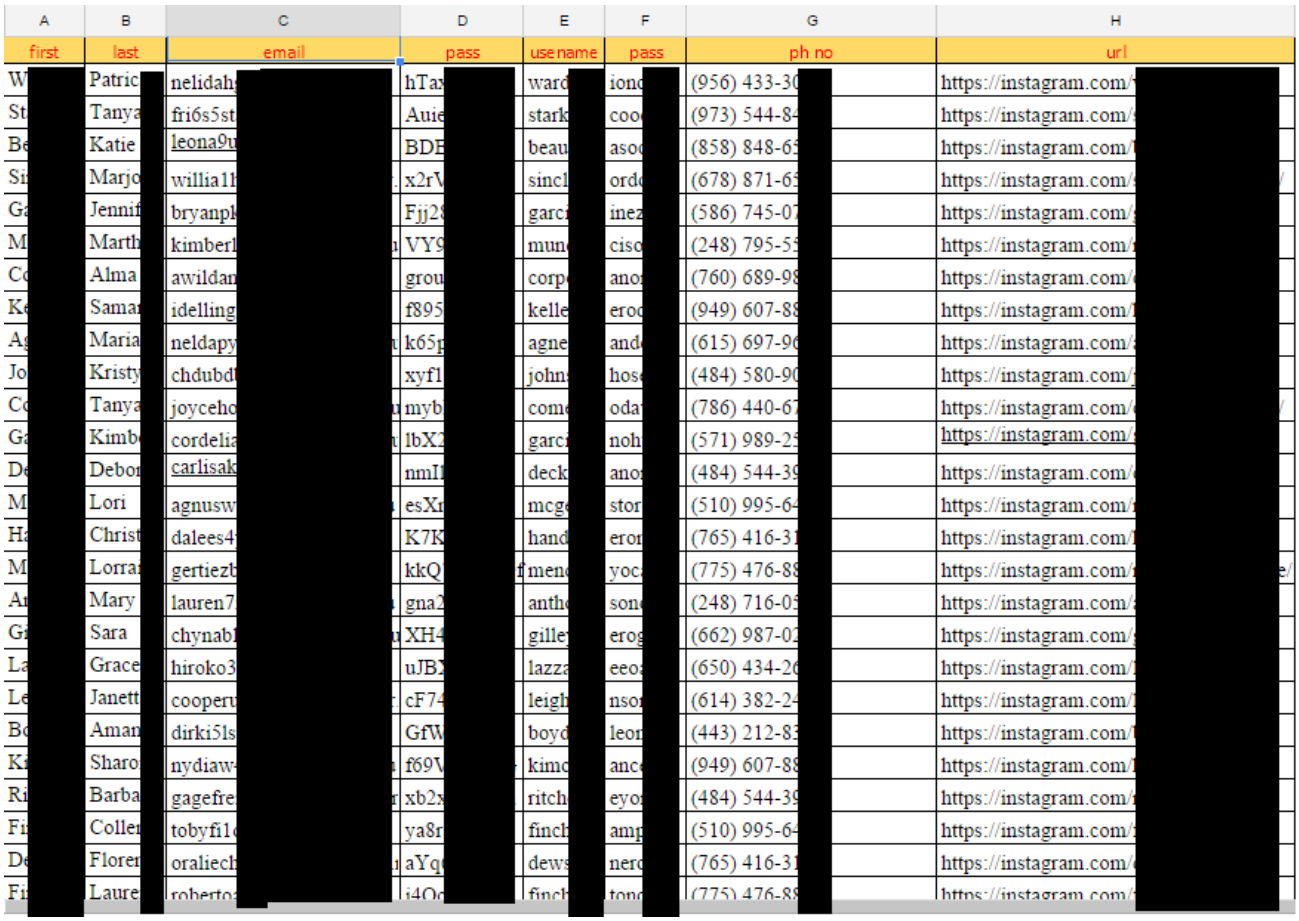
	Tot. new Followers	Tot. new Posts
March 18-20	687817	146958
April 11-13	327076	67556

14.Interesting data about botnets

As mentioned earlier, managing a botnet is not an easy task and requires some technical expertise. This includes a management software, account verification via email and very often via mobile phone, and a high quality proxy – along with, again, a skilled technical knowledge.

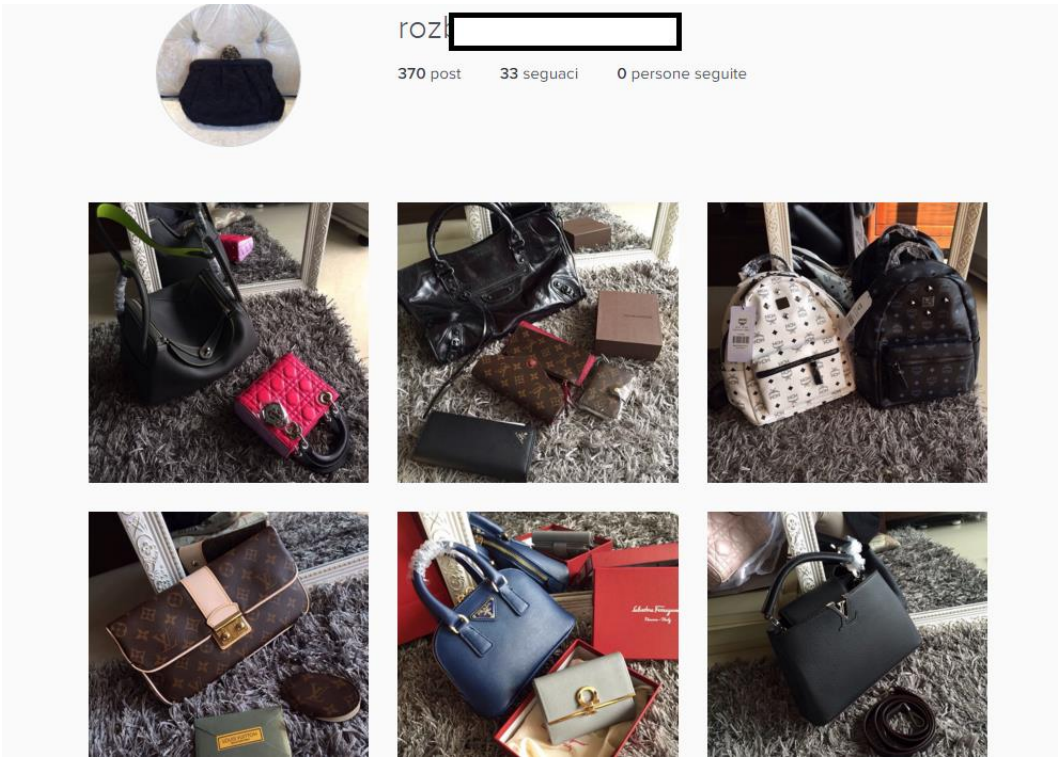
Therefore we decide to highlight some features related to the active botnets.

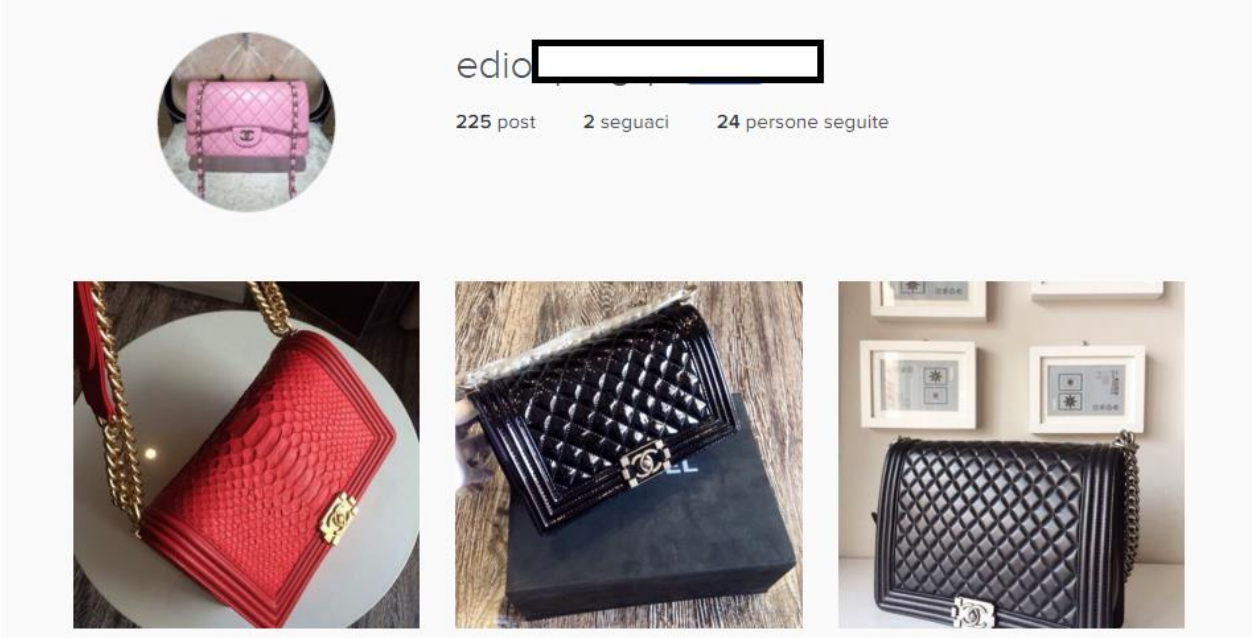
Here below is a list of Instagram accounts produced by a software program and verified through their email addresses and mobile phone numbers.



A	B	C	D	E	F	G	H
first	last	email	pass	username	pass	ph no	url
W[redacted]	Patric[redacted]	nelidah[redacted]	hTa[redacted]	ward[redacted]	ion[redacted]	(956) 433-30	https://instagram.com/[redacted]
St[redacted]	Tanya[redacted]	fri6s5st[redacted]	Aue[redacted]	stark[redacted]	coo[redacted]	(973) 544-84	https://instagram.com/[redacted]
Be[redacted]	Katie	leona9u[redacted]	BDE[redacted]	beau[redacted]	aso[redacted]	(858) 848-65	https://instagram.com/[redacted]
Si[redacted]	Marjo[redacted]	willia1l[redacted]	x2rV[redacted]	sincl[redacted]	ord[redacted]	(678) 871-65	https://instagram.com/[redacted]
Ga[redacted]	Jennif[redacted]	bryanpk[redacted]	Fjj28[redacted]	garci[redacted]	inez[redacted]	(586) 745-07	https://instagram.com/[redacted]
M[redacted]	Marth[redacted]	kimberl[redacted]	VY9[redacted]	mun[redacted]	cisc[redacted]	(248) 795-55	https://instagram.com/[redacted]
Co[redacted]	Alma	awildan[redacted]	grou[redacted]	corp[redacted]	ano[redacted]	(760) 689-98	https://instagram.com/[redacted]
Ke[redacted]	Samar[redacted]	idelling[redacted]	f895[redacted]	kelle[redacted]	erod[redacted]	(949) 607-88	https://instagram.com/[redacted]
Ag[redacted]	Maria[redacted]	neldapy[redacted]	k65p[redacted]	agne[redacted]	and[redacted]	(615) 697-96	https://instagram.com/[redacted]
Jo[redacted]	Kristy	chdubdt[redacted]	xyf1[redacted]	john[redacted]	hos[redacted]	(484) 580-90	https://instagram.com/[redacted]
Co[redacted]	Tanya[redacted]	joyceho[redacted]	myb[redacted]	come[redacted]	oda[redacted]	(786) 440-67	https://instagram.com/[redacted]
Ga[redacted]	Kimb[redacted]	cordelia[redacted]	lbX2[redacted]	garci[redacted]	noh[redacted]	(571) 989-25	https://instagram.com/[redacted]
De[redacted]	Debor[redacted]	carlisak[redacted]	nmI[redacted]	deck[redacted]	ano[redacted]	(484) 544-39	https://instagram.com/[redacted]
M[redacted]	Lori	agnusw[redacted]	esXr[redacted]	mcge[redacted]	stor[redacted]	(510) 995-64	https://instagram.com/[redacted]
Ha[redacted]	Christ[redacted]	dalees4[redacted]	K7K[redacted]	hand[redacted]	eron[redacted]	(765) 416-31	https://instagram.com/[redacted]
M[redacted]	Lorra[redacted]	gertiezb[redacted]	kkQ[redacted]	f[redacted]men[redacted]	yoc[redacted]	(775) 476-88	https://instagram.com/[redacted]
An[redacted]	Mary	lauren7[redacted]	gna2[redacted]	anth[redacted]	son[redacted]	(248) 716-05	https://instagram.com/[redacted]
Gi[redacted]	Sara	chynab[redacted]	XH4[redacted]	gille[redacted]	erog[redacted]	(662) 987-02	https://instagram.com/[redacted]
La[redacted]	Grace	hiroko3[redacted]	uJB2[redacted]	lazza[redacted]	eeo[redacted]	(650) 434-26	https://instagram.com/[redacted]
Le[redacted]	Janett	cooperu[redacted]	cF74[redacted]	leigh[redacted]	nso[redacted]	(614) 382-24	https://instagram.com/[redacted]
Bo[redacted]	Aman[redacted]	dirki5ls[redacted]	GfW[redacted]	boyd[redacted]	leon[redacted]	(443) 212-83	https://instagram.com/[redacted]
Ki[redacted]	Sharo[redacted]	nydiaw[redacted]	f69V[redacted]	kimc[redacted]	anc[redacted]	(949) 607-88	https://instagram.com/[redacted]
Ri[redacted]	Barba[redacted]	gagefre[redacted]	xb2x[redacted]	ritch[redacted]	eyo[redacted]	(484) 544-39	https://instagram.com/[redacted]
Fi[redacted]	Colle[redacted]	tobyfi1[redacted]	ya8r[redacted]	finch[redacted]	amp[redacted]	(510) 995-64	https://instagram.com/[redacted]
De[redacted]	Flore[redacted]	oraliech[redacted]	aYq[redacted]	dews[redacted]	nerc[redacted]	(765) 416-31	https://instagram.com/[redacted]
Fi[redacted]	Laure[redacted]	roberto[redacted]	i4Oc[redacted]	finch[redacted]	tond[redacted]	(775) 476-88	https://instagram.com/[redacted]

The following screenshots originate from two powerful Chinese botnets, including 243 bots (A) and 242 bots (B), respectively:



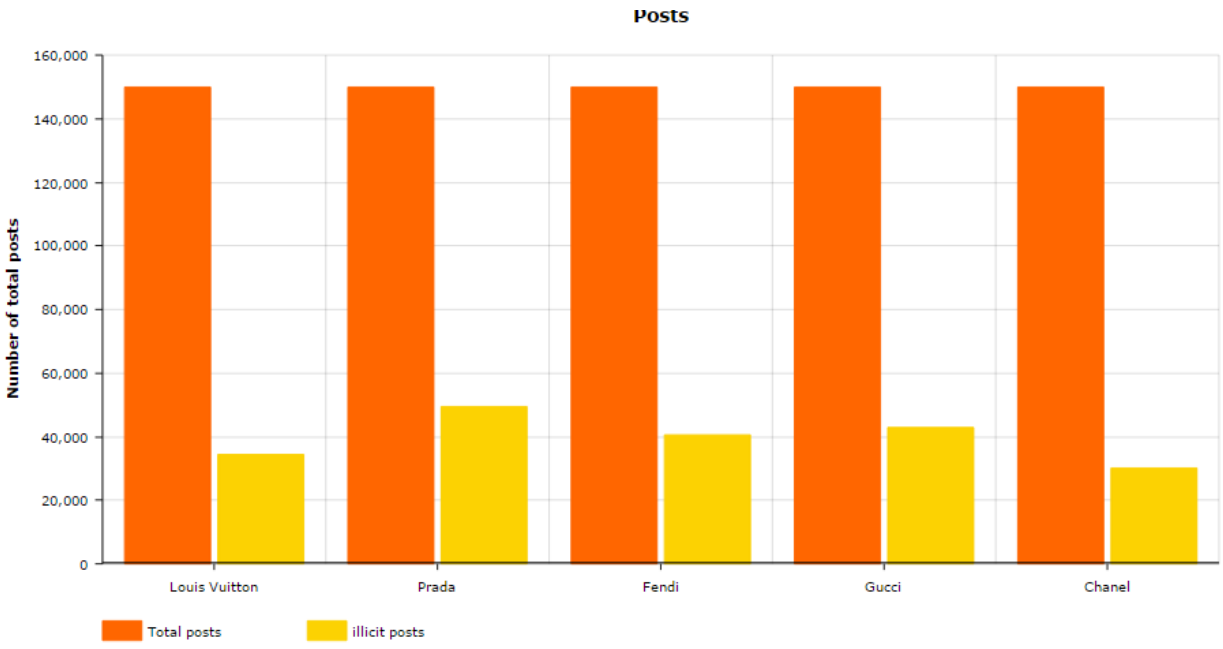


These botnets also show important figures about their total followers and posts, with a broader effect on potential viewers and customers. They were able to post the considerable sum of 117,000 ads about counterfeit and fake items without being detected by neither Instagram managers nor law enforcement patrolling.

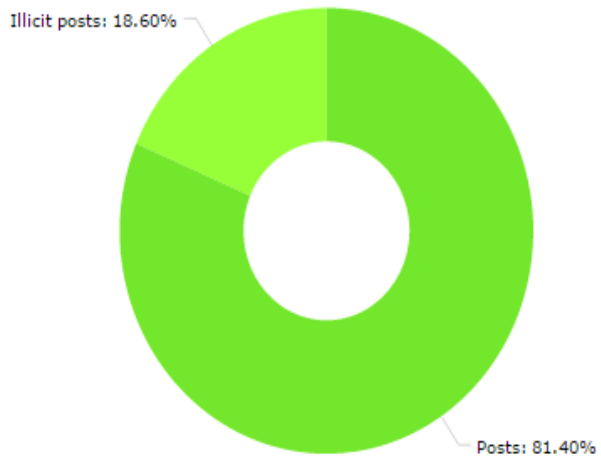
	Tot. followers	Tot. posts
Botnet A	14237	86783
Botnet B	6192	30910

15. Illicit posts and hashtag search

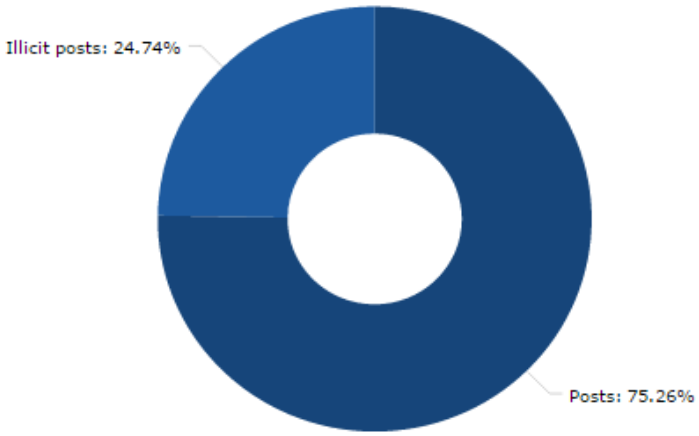
Instagram provide powerful search options that enable to locate a specific name, hashtag or content posted on the entire platform. We looked up over 150,000 illicit posts for five different hashtags, related to most popular fashion brands, (#LouisVuitton, #Prada, #Fendi, #Gucci, #Chanel). As shown in the image below, between 30,000 and 50,000 of total illicit posts included at least one of these hashtags.



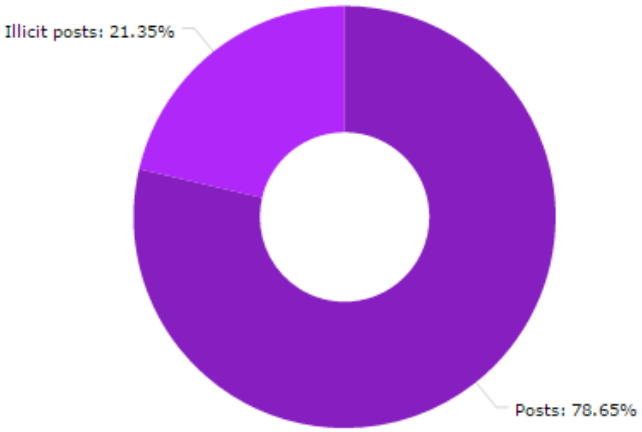
Here below the specific pie charts for each hashtag:



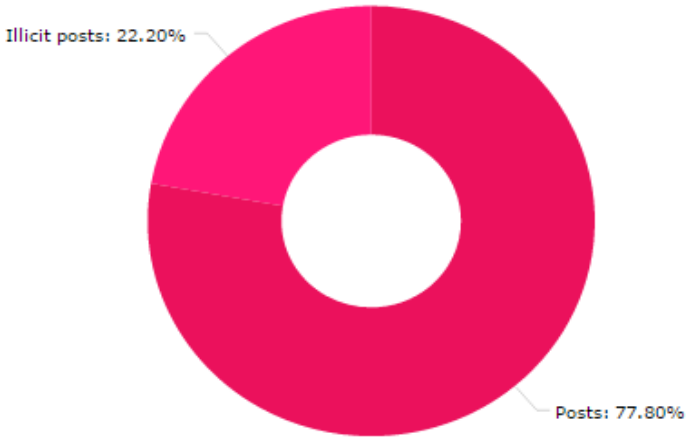
Louis Vuitton



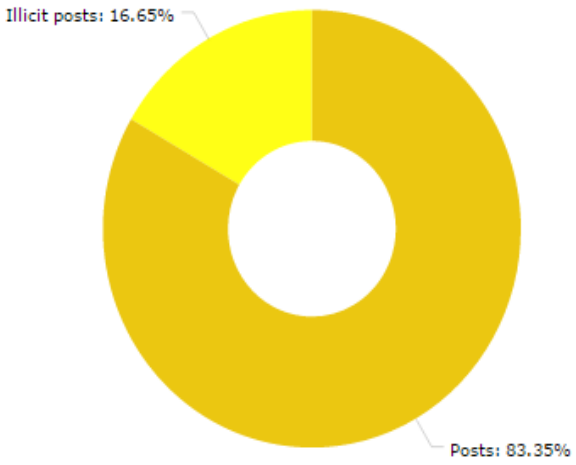
Prada


Illicit posts: 21.35%
Posts: 78.65%

Fendi


Illicit posts: 22.20%
Posts: 77.80%

Gucci



Chanel

When combined, the above charts show that about 20% of these posts feature counterfeit items. More interestingly, most accounts selling counterfeit merchandise upload a large quantity of posts every day, resulting in a chaotic and negative user experience. Instead of exploring the latest trends in fashion, or looking for catching images of boys and girls enjoying their recent purchase, you are facing a flashy and chaotic bazaar of illicit ads – thus increasing the chances that eventually you end up by clicking on a counterfeit item.

16.The need for advanced detection systems

As shown above, these dynamic and innovative techniques make harder and harder to detect an account or seller of fake luxury items on Instagram (and other social media platforms). This is particularly true when user profiles or

images provide very few (or none) details. Indeed, many image are embedded not only with a series of hashtags but also with seller contact info and item final price.

This is a clever strategy to bypass Instagram's detection algorithm, unable to differentiate such tiny details in a picture. Fortunately, new technologies are now able to detect these details with a certain precision, based on Optical Character Recognition (OCR) software, as shown in the following example[30]

It should be noted, though, that these counterfeit sellers are quick to deploy their counter-strategies: as shown in previous images, some of those embedded words are slightly out of focus. Another smart attempt to elude even the most sophisticated OCR software.

17. A difficult law-enforcement issue for Instagram

To ward off this broad wave of fake accounts and bots, Instagram deployed several new measures after the

[30] https://ocr.space/

December 2014 cleansing process. We also noticed on-going automatic and manual "patrolling" to locate and block spam bots, along with larger internal efforts coordinated by software engineers. It remains to be seen, though, if and how these measures will actually prevent such a widespread trend permanently. Indeed, it was no mystery online that many bots were able to "survive the great Instagram spam purge". Maybe the only solution will be for Instagram to purge its site again and again, expecting only to temporarily discourage spammers. Below is a summary of some of the counter-measures implemented on Instagram after this first wave of "dangerous accounts" was exposed.

Action	Detection technique	Counter-measure
Mapping	Account makes over X actions per hour	Temporary ban
Mapping	Account originates every time from different IP	Temporary ban
Botnet Action	Several accounts from same device	New account ban
Botnet Action	Account originates from confirmed spamming IP	IP ban
Botnet Action	Suspicious IP with email addresses on major providers (Gmail/Yahoo,Hotmail)	Account confirmation, if failed, IP ban

In any case, the sales of counterfeit items particularly on the popular photo-sharing platform have increased multifold in recent months, and as a matter of fact Instagram doesn't seem equipped well enough to effectively block this overgrown trend. The above mentioned counter-measures (especially blocking posts that include famous brand hashtags) can discourage sellers just temporarily, while penalizing also actual users that can only display the "most popular" posts.

For example, here below are three photos with three blocked hashtags (Dior, Bvlgari, Michael Kors).

Recent posts from #dior are currently hidden because the community has reported some content that may not meet Instagram's community guidelines. Learn more

ABOUT US SUPPORT BLOG PRESS API JOBS PRIVACY TERMS LANGUAGE

© 2016 INSTAGRAM

Recent posts from #bvlgari are currently hidden because the community has reported some content that may not meet Instagram's community guidelines. Learn more

ABOUT US SUPPORT BLOG PRESS API JOBS PRIVACY TERMS LANGUAGE

© 2016 INSTAGRAM

18.Conclusion

The online market of counterfeit and fake luxury goods is clearly on the rise. Unstoppable as it seems, this trend is having a negative impact on our societies at large. Unfortunately, this is hardly a breaking news. Often we dismiss this phenomenon as an unavoidable consequence of our modern life, along with terrorism, illegal drug trade, weapon trafficking and so on. However, this kind of "market" is not to be taken lightly. Its ramifications and connections are getting deep in every sector of today's economy. Its long tail is having very negative outcome at intellectual, social and cultural level. In the meantime, its varied activities are becoming more sophisticated and effective day by day, taking full advantage of social media penetration and our always-on lifestyle. But we still need to understand its full scope and effect in order to properly address it and find adequate solutions at both National and global levels.

Our research reveals that a big shift is taking place the (online) world of counterfeiting. After all, one fifth of our 750,000 posts (20%) about top fashion brands features counterfeit and/or illicit products. A percentage that could easily grow multifold in a short time. Indeed, these sellers are no longer hidden in some far-away "souks" or confined in a rough neighborhood market. They operate "in the open", posting a wide range of ads and images on social media and openly selling their goods worldwide. Today there is almost a direct line between "producers" and consumers with no filter or barrier of any sort. The internet is being used as a giant amplifier to attract more customers and finalize their orders. Then an international carrier service will deliver the "original" goods on their front door. Just like any legitimate global economy.

This new wave of cyber-vendors is technology-savvy: they use secure mobile apps Telegram or Whatsapp, create fake websites almost identical to those of famous brands, deploy botnets to bypass internal security systems, post thousands of images daily, and so forth. And when an account (or botnet) is exposed and blocked by Instagram or WeChat, it pops again under a new nick in a matter of days or even hours. The same goes for a suspicious website: if caught and banned, it resurfaces hosted on another ISP (or even country) at amazing speed.

Even with such level of complexity, this business structure reveals its weak spots. Of course, there is no way to prevent the on-going production and sales of counterfeit goods, particularly within certain countries. A possible

solution is instead trying to intervene at the level of the local amplifiers, that is, social media platform and IM apps. These entities should develop adequate technical filters, deploy human resources and provide better management. Cyber-cops and smart policing are also needed. Users should be more aware and be careful in avoiding such scams. In other words, we must set up a coordinated, global strategy including all various stakeholders.

Based on data and information explained above, this strategy should focus on some crucial key-points: developing and applying specific detection technologies (including the promising blockchain options), based on a working group similar to Facebook's ThreatExchange; direct involvement of and open info-sharing among producers, authorities, hi-tech companies, consumer associations and other pertinent organizations (maybe through an international communication center); entrust think-tanks and experts to come up with ad hoc policies and broader initiatives for the long term; introduce new ways to verify legitimate e-commerce individuals and companies; promote a broader user awareness on this issue with public campaigns and other initiatives, both online and on the ground.

In conducting our research, we met with representatives of major fashion companies: they were very angry and frustrated about this unstoppable trend of online counterfeiting and its related damages. We talked with different organizations and even with some doctors: they have pointed out that the lack of control and bad quality of cosmetics and other products is quite harmful to our health. Not to mention an overall loss of income for businesses and taxes to state coffers, a general loss of jobs and long-term problems for several industries – coupled with other indirect damages to our societies, well beyond the internet-sphere. In studying this phenomenon, we managed to highlight some new strategies of today's online counterfeit world. We believe that these data can actually help institutions and companies to implement a smarter operative model to prevent such trafficking, or at lest to considerably curtail it. We cannot forget that, in many instances, this illegal market is a driving force for organized crime, exploitation of children, and even financing of terrorism. As for other global challenges that are facing us, this new surge of online counterfeit activity requires a comprehensive strategy and a cross-sector collaboration. Sooner rather than later.