

Classiscam expands to Europe: Russian-speaking scammers lure Europeans to pages mimicking classifieds

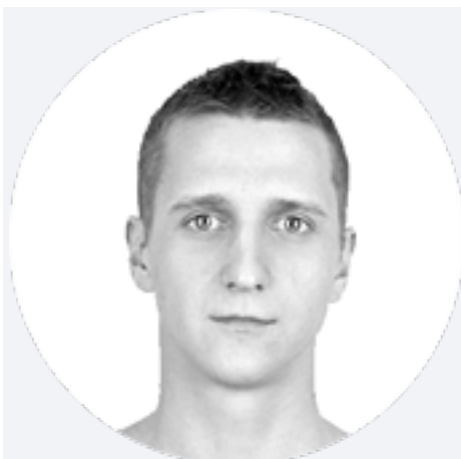
Group-IB, a global threat hunting and adversary-centric cyber intelligence company, has discovered that Russian-speaking scammers started targeting users of European marketplaces and classifieds. The scheme, dubbed Classiscam by Group-IB, is an automated scam as a service designed to steal money and payment data. The scheme uses Telegram bots that provide scammers with ready-to-use pages mimicking popular classifieds, marketplaces and sometimes delivery services. According to Group-IB, over 20 large groups, leveraging the scheme, currently operate in Bulgaria, the Czech Republic, France, Poland, Romania, the US, and post-Soviet countries, while 20 more groups work in Russia. These 40 groups altogether made at least USD 6.5 mln in 2020. Scammers are actively abusing brands of popular international classifieds and marketplaces, such as Leboncoin, Allegro, OLX, FAN Courier, Sbazar, and etc. Group-IB has sent notifications to the affected brands so they could take the necessary steps to protect against Classiscam.

The scheme, which initially exploited delivery brands, has been tried and tested in Russia. Analysts warn that it is now growing rapidly and reaching users of European classifieds and marketplaces, which were chosen as a target by Russian-speaking scammers to increase their profits and reduce the risk of being caught. Fighting the scam requires joint efforts by classifieds, marketplaces, and delivery services. It is also key to use advanced digital risk protection technology to ensure that any brand impersonating attacks are quickly detected and taken down.

Exporting Classiscam

[Group-IB Computer Emergency Response Team \(CERT-GIB\)](#) for the first time recorded the Classiscam in Russia in the summer of 2019. Peak activity was recorded in the spring of 2020 due to the massive switch to remote working and an increase in online shopping.

In the summer of 2020 we took down 280 scam pages as part of the Classiscam scheme, and by December that number grew 10-fold and reached up to 3,000 pages. We see that Classiscammers are now actively migrating from Russia to Europe and other countries. It's not the first time when Russia serves as a testing ground for cybercriminals with global ambitions.



Yaroslav Kargalev

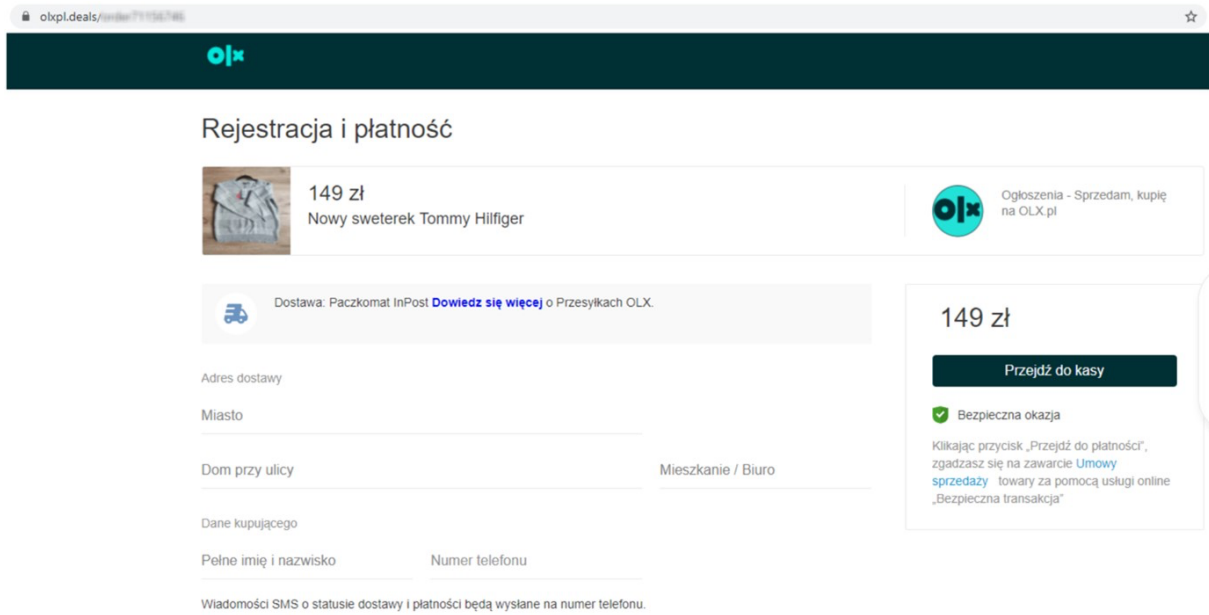
CERT-GIB deputy head



Group-IB's [Digital Risk Protection](#) and CERT-GIB experts have so far identified at least 40 active Classiscam gangs that use scam pages mimicking popular classified, marketplace, and delivery companies with every one of them running a separate Telegram bot. Half of the groups already operate outside of Russia. Despite that scammers are making their first attempts in Europe, an average theft costs users about USD 120. The scam was localized for the markets of Eastern and Western Europe. The brands abused by scammers include the French marketplace Leboncoin, Polish brand Allegro, Czech site Sbazar, Romanian FAN Courier, DHL and many others. An analysis of underground forums and chats revealed that scammers are getting ready to use new brands in their scams, these are FedEx and DHL Express in the US and Bulgaria.


As part of the scheme, scammers publish bait ads on popular marketplaces and classified websites. The ads usually offer cameras, game consoles, laptops, smartphones, and similar items for sale at deliberately low prices. The buyer


contacts the seller, who lures the former into continuing the talk through a third party messenger, such as WhatsApp. It's noteworthy that scammers pose as both buyers and sellers. To be more persuasive, the scammers use local phone numbers when speaking with their victims. Such services are offered in the underground.




obxpl.deals/offer/71156746

Rejestracja i płatność

 **149 zł**
Nowy sweterek Tommy Hilffiger

 Ogłoszenia - Sprzedam, kupię na OLX.pl

 Dostawa: Paczkomat InPost [Dowiedz się więcej](#) o Przesyłkach OLX.

Adres dostawy

Miasto

Dom przy ulicy Mieszkanie / Biuro


Dane kupującego

Pełne imię i nazwisko Numer telefonu

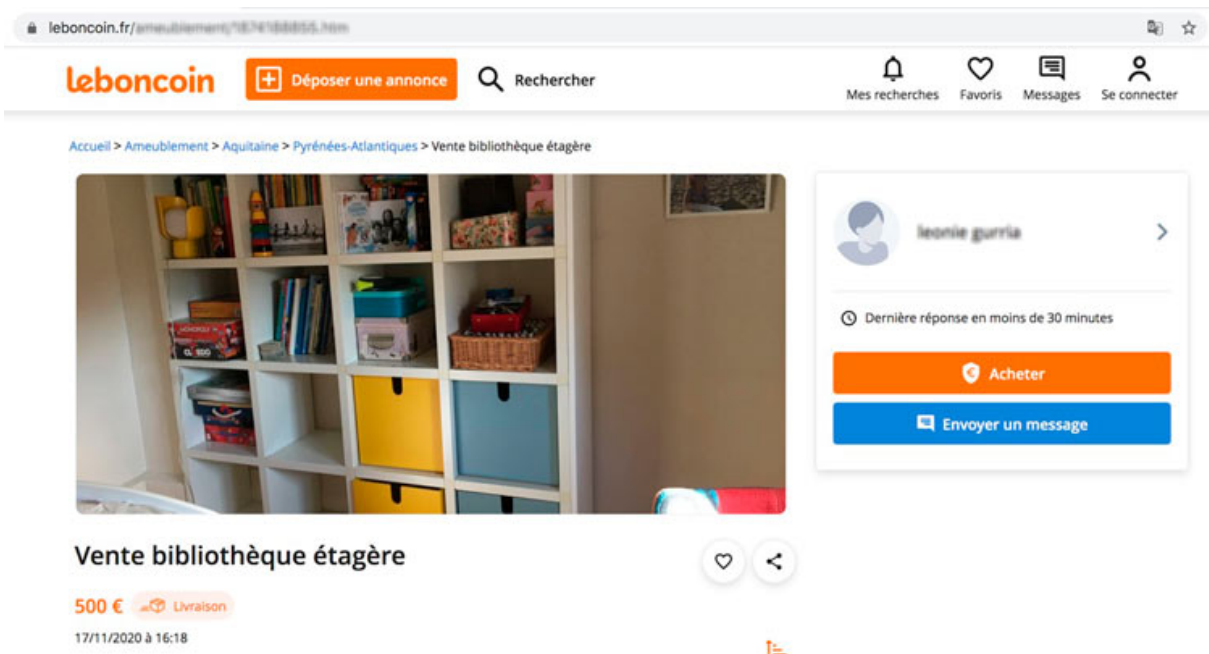
Wiadomości SMS o statusie dostawy i płatności będą wysłane na numer telefonu.

149 zł

Przejdź do kasy

 **Bezpieczna okazja**

Klikając przycisk „Przejdź do płatności”, zgadzasz się na zawarcie [Umowy sprzedaży](#) towaru za pomocą usługi online „Bezpieczna transakcja”





leboncoin.fr/ameublement/1874188855.htm


leboncoin [+ Déposer une annonce](#) [Rechercher](#)

Mes recherches Favoris Messages Se connecter

Accueil > Ameublement > Aquitaine > Pyrénées-Atlantiques > Vente bibliothèque étagère




 leonie gurria >

 Dernière réponse en moins de 30 minutes

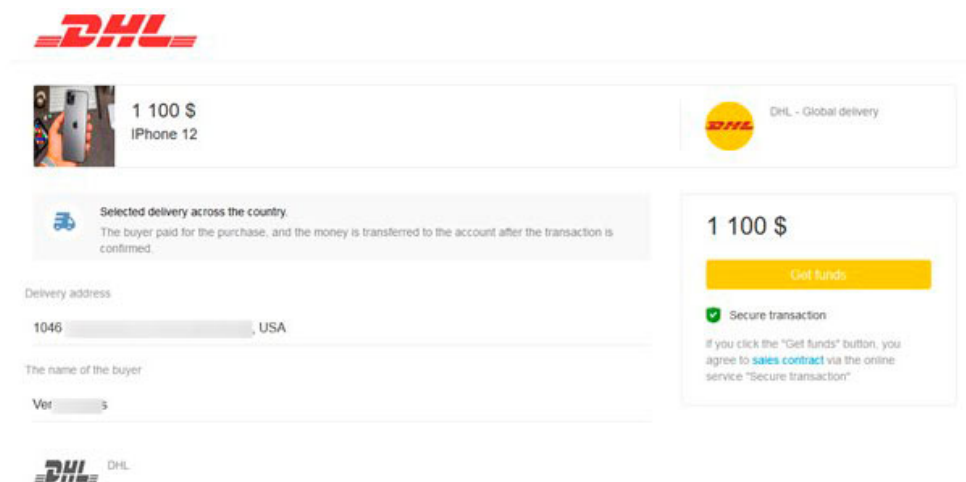
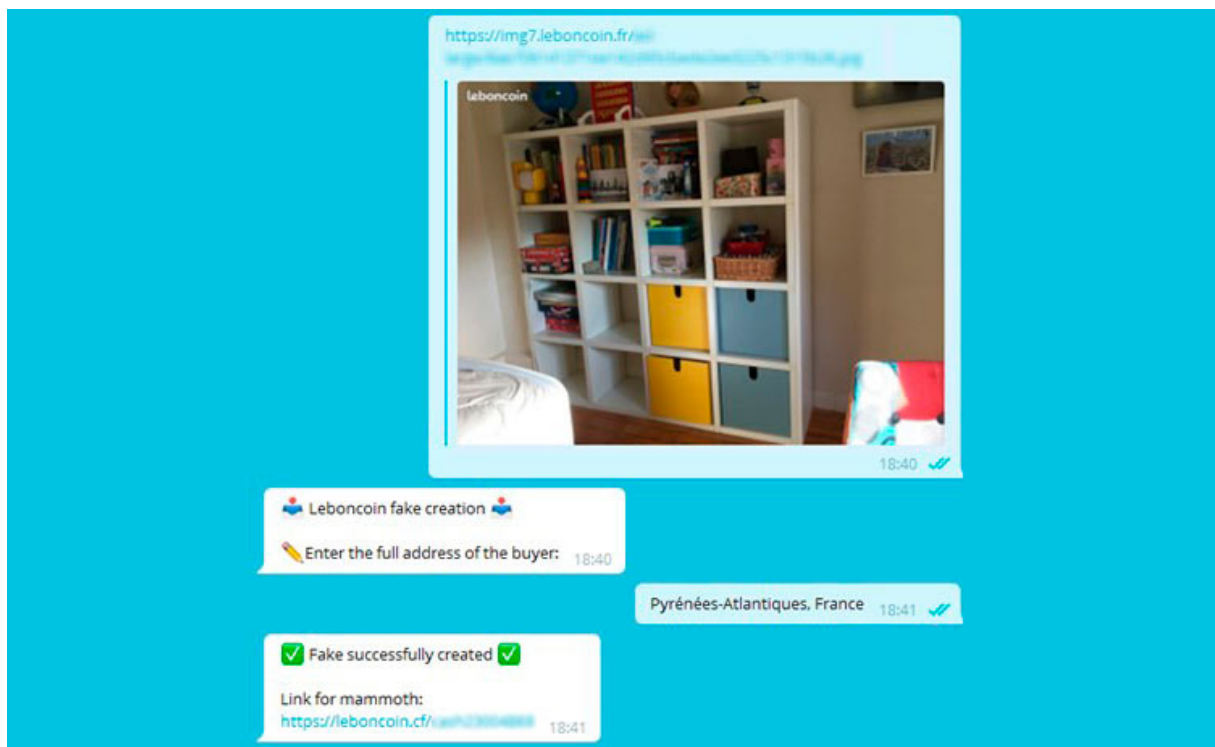
Acheter

Envoyer un message

Vente bibliothèque étagère

500 €  Livraison

17/11/2020 à 16:18



Although many marketplaces and classifieds that sell new and used goods have an active policy of protecting users from fraudsters by posting warnings on their resources, victims continue to give away their data.

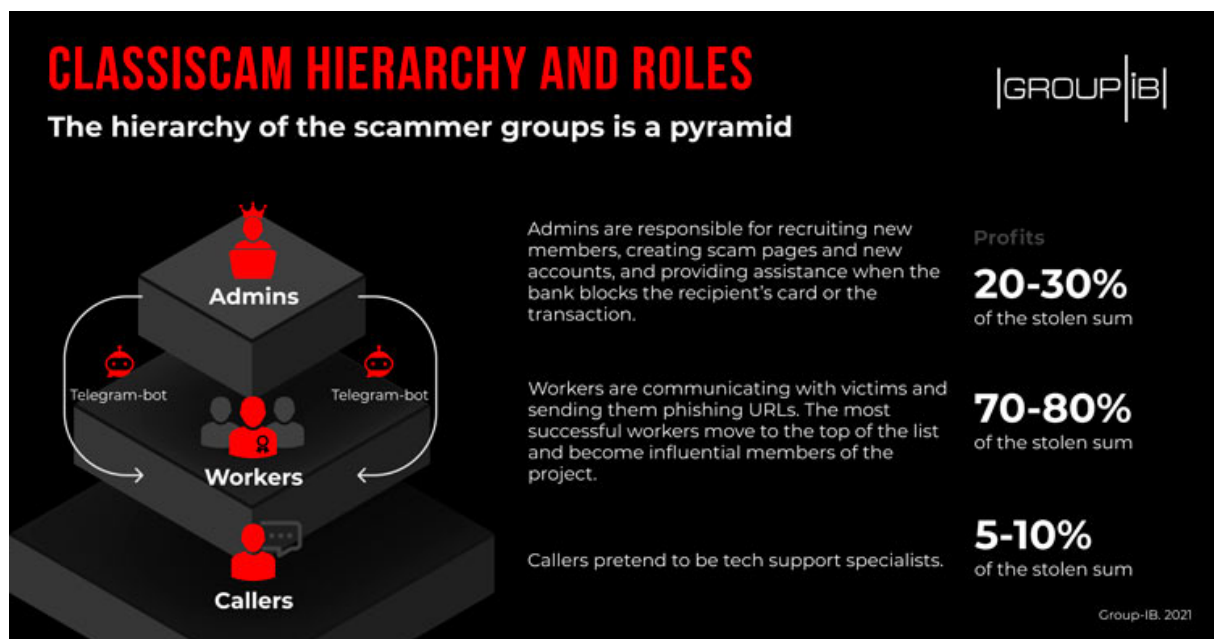
Evildoers ask victims to provide their contact information to allegedly arrange a delivery. The scammer then sends the buyer an URL to either a fake popular courier service website or a scam website mimicking a classified or a marketplace with a payment form, which turns out to be a scam page. As a result, the fraudster obtains payment data or withdraws money through a fake merchant website. Another scenario involves a scammer contacting a legitimate seller under the guise of a customer and sending a fake payment form mimicking a marketplace and

obtained via Telegram bot, so that the seller could reportedly receive the money from the scammer.

Classiscam Hierarchy

Group-IB discovered at least 40 groups leveraging Classiscam, with each of them running a separate Telegram chat-bot. At least 20 of these groups focus on European countries. On average, they make around US \$61,000 monthly, but profits may differ from group to group. It is estimated that all 40 most active criminal groups make US \$522,000 per month in total.

The hierarchy of the scammer groups represents a pyramid, with the topic starters on top. They are responsible for recruiting new members, creating scam pages, registering new accounts, and providing assistance when the bank blocks the recipient's card or the transaction. The topic starters' share is about 20-30 percent of the stolen sum. «Workers» get 70-80 percent of the stolen sum for communicating with victims and sending them phishing URLs.



All details of deals made by workers (including the sum, payment number and username) are displayed in a Telegram bot. That's how Group-IB experts were able to calculate their estimated monthly haul.

Based on payment statistics, the most successful workers move to the top of the list and become influential members of the project. By doing so, they gain access to VIP options in the chats and can work on European marketplaces, which offer a higher income and involve less risks for Russian-speaking scammers. Workers'

assistants are called «callers» and «refunders.» They pretend to be tech support specialists and receive 5-10 percent of the revenue.

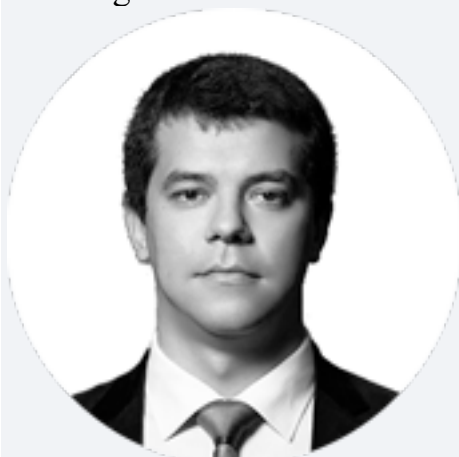
Phishing kit in Telegram

The scheme is simple and straightforward, which makes it all the more popular. There are more reasons behind its growing popularity, however, such as automated management and expansion through special Telegram chat bots. More than 5,000 users (scammers) were registered in 40 most popular Telegram chats by the end of 2020.

As it stands, workers just need to send a link with the bait product to the chatbot, which then generates a complete phishing kit including courier URL, payment, and refund. There are more than 10 types of Telegram bots that create scam pages for brands from Bulgaria, the Czech Republic, France, Poland, and Romania. For each brand and country, scammers write scripts that help newbie workers log in to foreign sites and communicate with victims in the local language.

Chatbots also have shops where you can purchase accounts to various marketplaces, e-wallets, targeted mailings, and manuals, or even hire a lawyer to represent you in court.

So far, the scam's expansion in Europe is hindered by language barriers and difficulties with cashing out stolen money abroad. Once the scammers overcome these barriers, Classiscam will spread in the West. The downside of popularity is competition among scammers, who sometimes frame each other without knowing it.



Dmitry Tiunkin

Deputy Director of Anti-Piracy and Brand Protection at Group-IB

HOW TO FIGHT CLASSISCAM

recommendations for brands

|GROUP|IB|



The detection of fraud at an early stage

Outsource the protection of your digital business assets to Digital Risk Protection technologies and Group-IB's team of experts.



The elimination of the threat

The complete elimination of adversary infrastructures at the stage when resources are being prepared to attack your brand and customers.



An 85% pre-trial takedown rate

The mitigation of risks on a pre-trial basis without additional investment and lengthy litigation.

Group-IB. 2021

Fighting the Classiscam

In order to protect their brands from Classiscam, companies need to go beyond the simple monitoring and blocking approach. Instead, it is necessary to identify and block adversary infrastructure using AI-driven digital risk protection systems enriched with data about adversary infrastructure, techniques, tactics, and new fraud schemes.

The recommendations for users are quite simple and include:

- Trust only official websites. Before entering your login details and payment information, double check the URL and Google it to see when it was created. If the site is only a couple of months old, it is highly likely to be a scam or a phishing page.
- When using services for renting or selling new and used goods, do not switch to messengers. Keep all your communication in the official chat.
- Do not order goods or agree to deals involving a prepaid transaction. Pay only after you receive the goods and make sure that everything is working properly.
- Large discounts and unbelievable promotions may be just that: too good to be true. They are likely to indicate a bait product and a phishing page. Be careful.