Analysis of Online Marketplace Scams

Mihai COTITU
General Inspectorate of the Romanian Police, Crime Research and Prevention Institute,
Research Department, Bucharest, Romania
mihai.cotitu@politiaromana.ro

Abstract

One of the many effects of the Covid-19 pandemic was reflected in the accelerated migration of many face-to-face activities towards the online environment, with online trading experiencing a significant growth during this period. At the same time, the risks specific to the digital environment have gone through a prosperous period. Thus, a telling example is given by the period August - December 2020, during which, at the level of the relevant authorities (D.I.I.C.O.T. and the Romanian Police) were registered approximately one thousand cases, based on cybercrime with similar modus operandi. These cases involved the collection of personal data through online resources, phishing, targeting in particular those who posted advertisements for the sale of objects through the OLX platform.

Index terms: classiscam, cybersecurity, marketplace, scam, WhatsApp

1. Introduction

The current paper aims to describe a recent type of online scam that has occurred through online marketplaces, the methods used by the perpetrators and the ways victims were deluded, the final goal being to support and to prevent future offences. This research is based on the analysis of online marketplaces posts/ announcements and interviews with police officers.

In comparison with previous scams carried out through the Internet, in which case perpetrators targeted people seeking for goods/acquisitions, therefore potential clients, a new practice among the scammers was identified recently: victims were selected from the sellers, people seeking to sell a product through an online marketplace.

In close connection with this reverse action (the perpetrator being the supposed customer/ buyer) the modus operandi is characterized by the eagerness to purchase and the lack of attention paid to the details of the good for sale. No details on the object of the transaction are required and no attempt is made to negotiate its value. Even if such requests (the reason for the sale, the request for a lower price) were made, they are rather of complacency and are limited to a single exchange of a limited number of inquiries.

2. How it works

It should be noted that the negotiation between the two parties, in order to complete the transaction, occurs mainly or exclusively outside the dedicated chat platform of OLX[1], on communication channels such as WhatsApp or using a classic phone call. Another peculiarity of these

[1] OLX is an online platform (marketplace) dedicated to buying and selling goods and services.

cases is the rather accurate depiction of the marketplace, which might seem authentic to a regular internet user or to a person who does not pay particular attention to safety details. Thus, after the discussion, the victim was offered a link, apparently similar to those generated by the portal that we already mentioned, in which he or she filled in the data written on the card in order to, hypothetically, receive the money for the good that was being sold. It should be noted that these steps are abnormal for a sale, and are also an indicator of a low-level of knowledge regarding online transactions. In a brief period of time, usually immediately after the data was disclosed, the bank account connected to the card was emptied, either in multiple steps or in a single transaction. Moreover, these transactions do not attract the attention of the banks. Confronted with the requests to not validate the transactions on behalf of the victims, the banks would often refuse to block them, claiming there is no ground for the request unless a criminal investigation is open. The banks consider the victims willingly provided their data, and that is why the request does not represent a reason for blocking transactions. A new indication of the technological capacity of the perpetrators is given by the possibility of the latter to carry out the operation even if there is security solutions such as the 3D-secure code, without it being disclosed by the victim, but only issued for the purpose of the transaction. Please note that, in some cases, as a preliminary step to better aiming their criminal activities, the victims were being asked in advance for information regarding the balance available into the account.

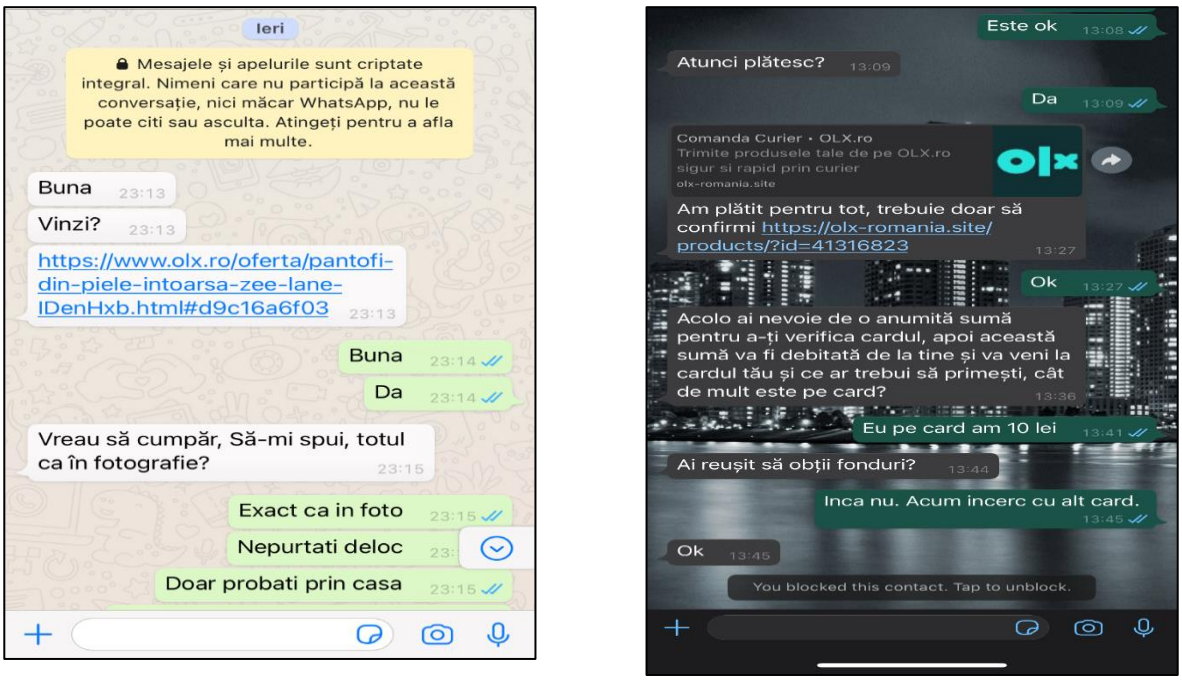


Fig. 1

As police workers also pointed out, the use of the previously mentioned channels (WhatsApp, classic call) makes the investigative steps more difficult. Moreover, criminals have the IT technique that allows the systematic alternation of telephone numbers through software that generate quickly random new numbers, beyond the simple method of purchasing and then disposal of pre-paid cards. Under these terms, the details regarding the author vary from file to file, the interception or location measures (geographical tracking) being either difficult to justify or imprecise, inconclusive.

The elements that may indicate the presence of organized crime cells are highlighted by situations in which the perpetrators have used classic telephone calls to contact the victims, on the opposite side of the call being a person who either tried to give the impression of the same nationality as the victim or had some training/practice to achieve this goal. Such a scenario may indicate the

willingness of criminals to gain some prior knowledge, or their ability to engage other people and hire collaborators. Therefore, the pecuniary benefits of this method, which allows payment to third parties, are also deducted. The use of the phone call was highlighted during the interviews with police officers, coming into contradiction with the previous elements that we had until then, that this type of offence is usually committed by foreign criminals. Previously, it was known that they preferred to communicate exclusively via WhatsApp, the language used not having the usual conversational fluency, indicating the possible use of an automated translation tool.

Fig. 2

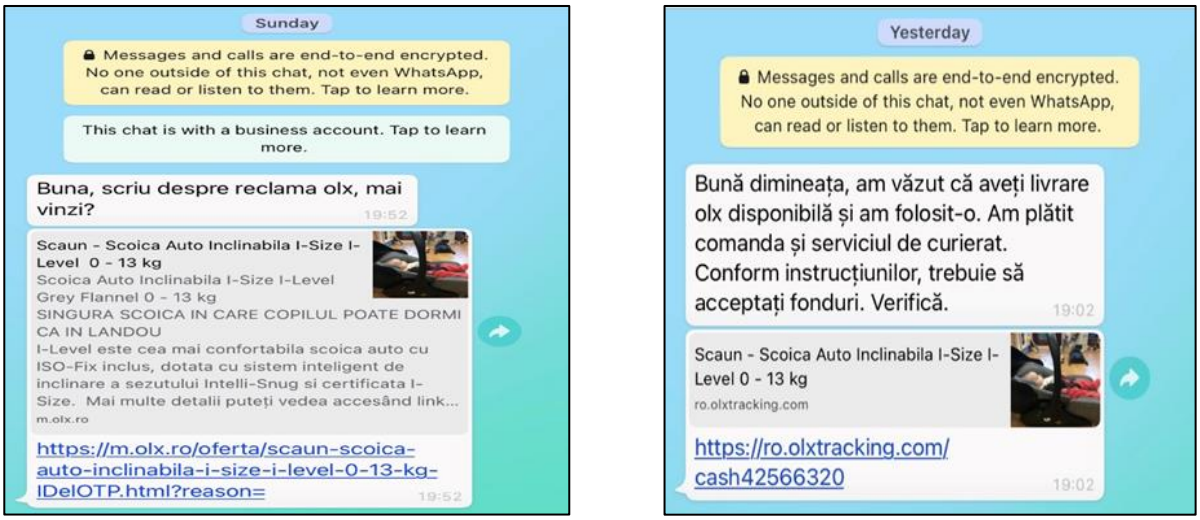


Fig. 3

Starting from this point, we cannot pass over the main weak spot of this equation: the victim and the need to inform her regularly about a minimum set of rules regarding online transactions, as well as about other undersupplied safety measures that users should adopt in order to have a positive online experience, highlighted by the investigative structures involved in resolving these cases (collaboration with the police, providing personal data). In educating the general public and in close connection with the perception of the state authority, we reiterate that, in some cases, the victims initially address CERT-RO, and the banks, but regarding the notifications submitted to police officers authorized to investigate these types of offences, they are reluctant to provide the data necessary for investigative activities and refuse to give out personal information, therefore they do not meet the requirements of Ordinance 27/2002 (on the regulation of petition settlement activities) or of the Order 33/2020 (on petition settlement activities, audience and counselling of citizens in the Ministry for Internal Affairs) and their notifications can be considered null, even though the initial form contains only some simple fields that are mandatory for the investigation to start.

In addition to the data presented above, as some users have reported their experiences in the online environment, new elements can be mentioned, such as:

- Scanning a QR code for the transaction, an action that does not involve forwarding the money to the seller, but giving up the value targeted by him;

- Payment already made by the alleged purchaser followed by the generation of a link in which the seller receives a confirmation that the requested amount of money has been transferred, but he is conditioned by the payment of a shipping fee;

Fig. 4

- The mentioning of another trading currency in the false link (e.g. rubles);

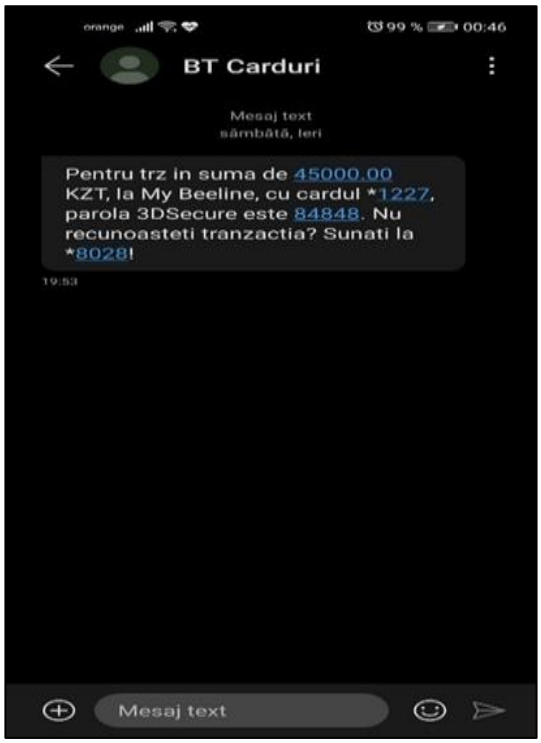


Fig. 5

- Being redirected to an alleged link belonging to a courier company;

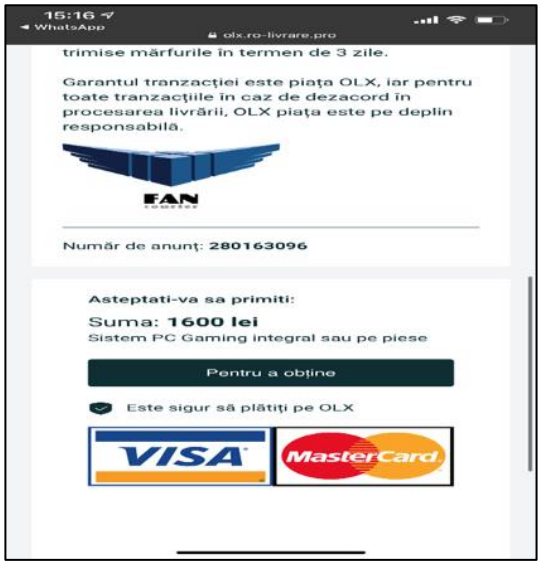
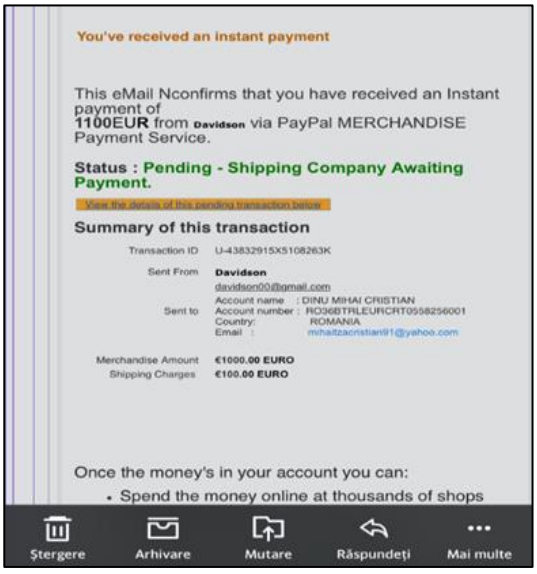


Fig. 6

- In order to create the impression of authenticity, in some cases, e-mails are sent imitating the brand elements of online payment companies.



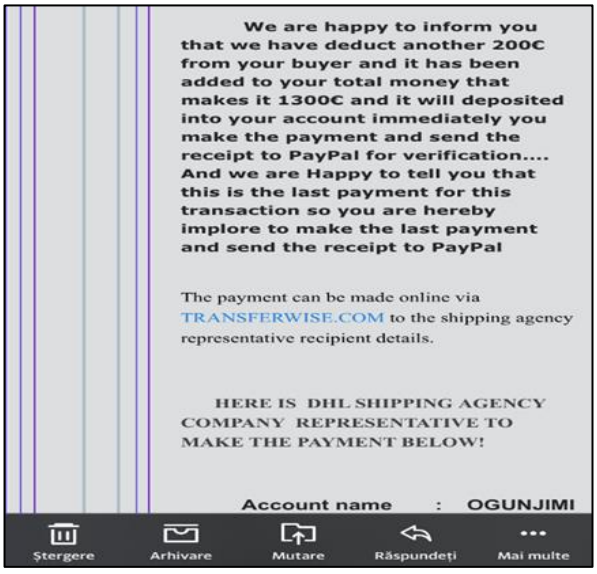


Fig. 7

Thus, in a predictive sense, these situations may be relevant for the possible variation of the scammer's way of action in the next period. CERT Poland issued warnings about ad platforms, through which text messages were issued to sellers prompting them to accept money. In fact, once approved, the money was being transferred to the offender's account, the operation being subsequent to the disclosure of card data. Returning to the national level, there is a reaction from the public to this scam, by posting on the targeted websites messages in which they would reveal their experiences with this type of scams and the people involved.

Focusing on the external context, even though the group that owns the OLX platform operates in several countries, national investigators did not receive information on similar cases from their

external counterparts. At the same time, they anticipate a perpetuation of phishing attempts, by using different platforms.

Comparing a series of online articles on similar topics, we find that similar practices have been encountered in other European countries (such as France, Poland, Bulgaria) as well as in much faraway countries (e.g. India). In the case of Poland, we can even speak of an overlap of the intensity of the facts, given the fact that the local branch of CERT issued a similar warning for the same platform, in October. This warning message also referred to a new method, in the way of issuing to the seller an alleged message approving the transaction, which in fact represented an agreement to withdraw that amount.

During the desk research, other reports indicated that there were more than 40 groups, especially from Russia, specialized in crimes involving the theft of personal data, especially banking data. Moreover, these reports issued a warning about the increase of these types of crimes, in parallel with the emergence of a new way of scamming, through false advertisements, a scam-as-a-service scheme. The presence of the attacks has been reported in a much larger number of countries, on a wider range of trading platforms.

Looking at the technical aspects of such crimes, the reports indicates that most offenders are based in Russia. After moving the conversation to another communication service (Telegram, WhatsApp) they use bots (programmed systems that can take over certain predefined tasks) to lead the victim to a link that mimics the format of certain websites, online marketplaces or delivery services, link necessary to take over bank credentials.

The method called Classiscam, involves an automated scam with the purpose of stealing money and bank credentials. They mainly use the portals or providers that are very popular on an international scale, such as: Leboncoin, Allegro, OLX, FAN Courier, Sbazar etc.

Specialists have identified about 40 groups of Russian origin using this technique, of which 20 operate in Bulgaria, the Czech Republic, France, Poland, Romania, the United States and in other states of the former Soviet Union, while another 20 groups focus strictly on Russia. According to estimates, their income was $ 6.5 million in the previous year, with an average per victim of $120, about $61,000 a month for each group, or a total of about $522,000 a month. In Russia, this type of scam was initially identified in the summer of 2019, but the peak was recorded in the spring of 2020, with the online migration of many activities. If 280 fake links were removed in the summer of 2020, the number grown to around 3,000 in December.

However, it is indicated that these attacks in Eastern and Western Europe are still in their infancy. In a predictive way, we can say that in the future, criminals will not rely heavily on "fake buyers" scenarios. Using the same portals, they will publish attractive ads (bait), displaying various electronics, and in order to create the illusion of authenticity, they will use phone numbers adapted to the local specifics of each country.

From an organizational point of view, the groups have a pyramidal hierarchy, headed by "administrators", followed by members who are dealing with recruitment, creating false links and managing some of the banking problems.

3. Keeping up with it

Over time, either through systematic progress or under the need to identify solutions in crisis situations, digitalization is becoming an integral part of several areas of our day-to-day activities.

Beyond acquiring these new ways of interacting with the online world, it is imperative to know the set of rules that will guide these new behaviours. In relation to/Regarding the online transactions

and the services provided by different online platforms, a collective approach is required both from the institutions involved in the investigation of these types of offences and from the private institutions whose clients or users may be affected.

Preventive measures are all the more necessary as, even if at the level of General Police Inspectorate of Romania there is a unit that manages this form of crime, at the territorial level the resources - from IT to the human one - are drastically limited.

These limitations place a favourable position, both in terms of accessibility and efficiency, of an information-awareness campaign carried out with the efforts of several actors, both from the private and public/state field.

References

[1]. I. Arghire, "Telegram-Based Automated Scam Service Helps Fraudsters Make Millions", securityweek.com, https://www.securityweek.com/telegram-based-automated-scam-service-helps-fraudsters-make-millions (Accessed on 20.02.2022).

[2]. "Classiscam expands to Europe: Russian-speaking scammers lure Europeans to pages mimicking classifieds," https://www.group-ib.com/media/classiscam-in-europe/ (Accessed on 18.02.2022).

[3]. J. Espinoza. "Digital payments deepen the threat of online fraud in Covid era". https://www.ft.com/content/d56bdbbb-f7f3-4b44-98c3-e1a372ed2280 (Accessed on 20.02.2022).

[4]. "Gang arrested for fraud on Olx: Everything you need to know about this 'big scam' while using Olx, Quikr". https://www.gadgetsnow.com/slideshows/gang-arrested-for-fraud-on-olx-everything-you-need-to-know-about-this-big-scam-while-using-olx-quikr/the-moment-you-post-your-ad-on-olx-or-quikr-you-will-get-a-call-from-a-prospective-buyer-in-many-cases-almost-immediately/photolist/75783800.cms (Accessed on 20.02.2022).

[5]. J. Jay. "Russian-speaking scammers tricking European shoppers using scam sites". teiss.co.uk. https://www.teiss.co.uk/news/russian-speaking-scammers-tricking-european-shoppers-using-scam-sites-8716 (Accessed on 20.02.2022).

[6]. H. Dugh. "Planning to sell stuff on OLX, Quikr? You might be cheated by fraudsters - Don't make these mistakes" https://www.zeebiz.com/personal-finance/news-planning-to-sell-stuff-on-olx-quikr-you-might-be-cheated-by-fraudsters-dont-make-these-mistakes-109014 (Accessed on 18.02.2022).

[7]. "Rising OLX fraud major concern for Gurugram Police" https://www.andhram.com/national/rising-olx-fraud-major-concern-for-gurugram-police/ (Accessed on 21.02.2022).

[8]. R. Jain. "Scammers are now using WhatsApp to steal money - here's how you can protect yourself". https://www.businessinsider.in/tech/apps/news/scammers-whatsapp-stealing-money-how-to-protect/articleshow/72976604.cms (Accessed on 20.02.2022).

[9]. "Telegram-Based Classiscam Operation Targeting Users of European Marketplaces". https://cyware.com/news/telegram-based-classiscam-operation-targeting-users-of-european-marketplaces-dd8d2183 (Accessed on 21.02.2022).

[10]. "The Mammoth Goes Abroad: Online Fraud Groups Move into the EU, US, and CIS". https://sk.ru/news/the-mammoth-goes-abroad/ (Accessed 18.02.2022).

[11]. T. Ankit. ”Don't fall prey to online scams on Paytm, WhatsApp and other popular apps”. https://www.wionews.com/Technology/Dont-Fall-Prey-To-Online-Scams-On-Paytm-Whatsapp-And-Other-Popular-Apps-337451 (Accesed on 19.02.2022).

[12]. ”Țeapă pe OLX! Cum a fost păcălită o ploieșteancă de un cumpărător din altă țară”. https://www.ziarulincomod.ro/teapa-pe-olx-cum-fost-pacalita-o-ploiesteanca-de-un-cumparator-din-alta-tara-foto/ (Accessed on 21.02.2022).