Scam-as-a-Service operation made more than $6.5 million in 2020

"Classiscam" operation is made up of around 40 groups operating in the US and across several European countries.

A newly uncovered Russian-based cybercrime operation has helped classified ads scammers steal more than $6.5 million from buyers across the US, Europe, and former Soviet states.

In a report published today, cyber-security firm Group-IB has delved into this operation, which the company has described as a Scam-as-a-Service and codenamed **Classiscam**.

According to the report, the Classiscam scheme began in early 2019 and initially only targeted buyers active on Russian online marketplaces and classified ads portals.

The group expanded to other countries only last year after they began recruiting scammers who could target and have conversations with foreign-language customers. Currently, Classiscam is active in more than a dozen countries and on foreign marketplace and courier services such as Leboncoin, Allegro, OLX, FAN Courier, Sbazar, DHL, and others.

How Classiscam operates

But despite the wide targeting, Classiscam's modus operandi follows a similar pattern —adapted for each site— and revolvs around publishing ads for non-existing products on online marketplaces.

"The ads usually offer cameras, game consoles, laptops, smartphones, and similar items for sale at deliberately low prices," Group-IB said today.

Once users are interested and contact the vendor (scammer), the Classiscam operator would request the buyer to provide details to arrange the product's delivery.

The scammer would then use a Telegram bot to generate a phishing page that mimicked the original marketplace but was hosted on a look-a-like domain. The scammer would send the link to the buyer, who would fill it with their payment details.

Once the victim provided the payment details, the scammers would take the data and attempt to use it elsewhere to purchase other products.

More than 40 Classiscam groups active today

Group-IB said that the entire operation was very well organized, with "admins" at the top, followed by "workers," and "callers."

Admins had the easiest job in the scheme, managing the Telegram bots, creating the fake ads, and recruiting "workers," both inside Russia and abroad.

Workers were the people who interacted with victims directly, doing most of the work, generating the individual phishing links, and making sure payments were made.

Callers had the smallest part in the scheme, acting as support specialists and having conversations with victims over the phone in case any suspected anything or had technical problems.

Based on the number of Telegram bots it discovered, Group-IB believes there are more than 40 different groups currently using Classiscam's services.

Half of the groups run scams on Russian sites, while the other half target users in Bulgaria, the Czech Republic, France, Poland, Romania, the US, and post-Soviet countries.

Group-IB said that more than 5,000 users (working as scammers) were registered in these 40+ Telegram chats at the end of 2020.

The security firm estimates that on average, each of these groups makes around $61,000/month, while the entire Classiscam operation makes around $522,000/month in total.

"So far, the scam's expansion in Europe is hindered by language barriers and difficulties with cashing our stolen money abroad," said Dmitriy Tiunkin, Head of Group-IB Digital Risk Protection Department, Europe. "Once the scammers overcome these barriers, Classiscam will spread in the West."

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.

References:

- https://www.zdnet.com/article/scam-as-a-service-operation-made-more-than-6-5-million-in-2020/?&web_view=true
- https://www.infosecurity-magazine.com/news/automated-classiscam-operation
- https://www.binarydefense.com/threat_watch/classiscam-operation-made-more-than-6-5-million-in-2020/