ESET Research white papers

Digital Security
Progress. Protected.

Marketplace scams:

Neanderthals hunting Mammoths with Telekopye

10 October, 2024

(eset):research

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Telekopye is a Swiss Army knife for turning online marketplace scams into an organized illicit business. Dozens of groups with up to thousands of members each utilize it every day to steal millions from Mammoths, as they call the targeted buyers and sellers. Neanderthals, as we call the scammers, require little to no technical knowledge – Telekopye takes care of everything in a matter of seconds.

Thanks to collaboration with law enforcement and several of the online marketplaces targeted by Telekopye, we were able to gain unique insight into the whole operation. One of the most shocking discoveries was that some Telekopye groups, instead of employing cybercriminal wannabes, threaten people in difficult life situations and force them to perform these scams. This chilling fact puts the whole operation into a completely different light. We were also able to better understand the online marketplaces' defense capabilities, and helped further strengthen their defenses based on what we learned from Neanderthals' internal documentation (obtained by infiltrating their ranks).

Telekopye is designed to target a large variety of services (OLX, Vinted, eBay, Wallapop), mainly in Europe and North America. It offers advanced features to its users – fully automated phishing webpage generation, an interactive chatbot with on-the-fly translation, and anti-DDoS protection of the whole phishing domain, to name a few.

Telekopye groups expanded their targeting recently – they added support for scam scenarios aimed at users of popular online platforms for hotel reservations. According to our telemetry, this scam type seems to be the most popular one currently. We will describe how this scenario works and how to detect and prevent it.

As the best defense against these scams is awareness, we will provide a comprehensive guide to evading the Neanderthals' spears.

INTRODUCTION

All of us have, from time to time, goods we don't really need, but also don't want to throw away since they might be useful for someone else. With the emergence of online marketplaces and their continuous growth, such platforms present a perfect solution. Sadly, besides buyers and sellers, there is another group who have their eyes set on online marketplaces – scammers.

Scams on these platforms are, unfortunately, a very common thing. Based on a *Besedo survey from 2024*, 40% of respondents have been scammed on online marketplaces. *Statista reports* that since 2015, every year over 70% of victims targeted by these scams lost money as a result, demonstrating the effectiveness of such scams. *Forbes reports* the average monetary loss in an e-commerce scam is $101. Finally, UK bank TSB *recently warned* that over a third of Facebook Marketplace adverts they tested could be scams.

How is it possible that online marketplace scams are so common and successful? And what can be done about it?

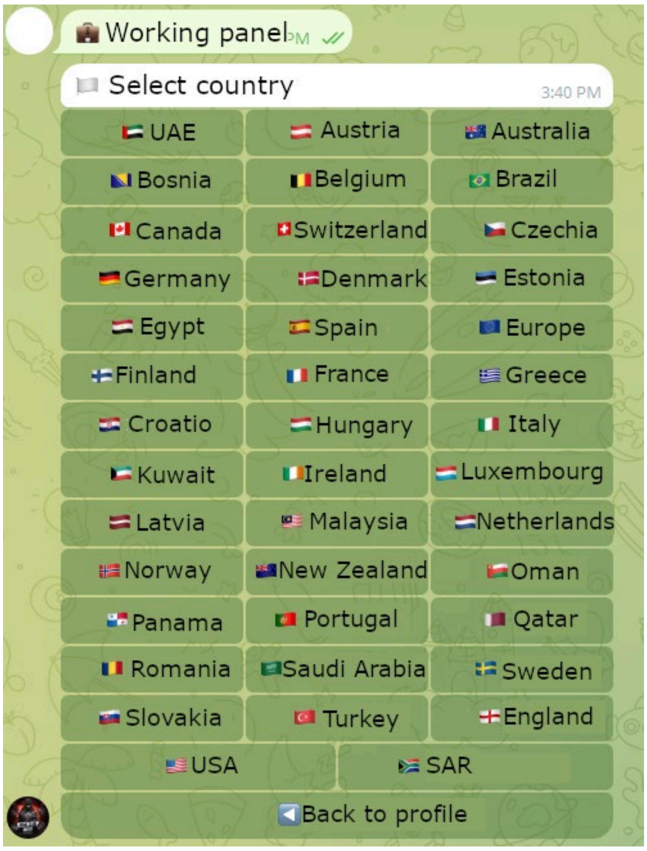
MEET TELEKOPYE

In 2023, ESET discovered a Telegram bot heavily utilized for online marketplace scams. It has been in use since at least 2016 and we have uncovered dozens of Telegram groups using it on a daily basis to scam victims all over the world, mainly in the EU and US. Multiple leads point to Russia as the country of origin of the bot's author(s) and also the scammers using it.

The scammers call their victims Mammoths, a common slang in Russian for someone you want to "screw over". Reversing this logic, we will refer to the scammers as Neanderthals. This ultimately led us to naming the bot Telekopye – a portmanteau of Telegram and kopye (копье), the Russian word for spear, both for its highly targeted (aka spear-) phishing and the fitting analogy with Pleistocene hunting.

Telekopye is written in PHP, allowing easy source code modifications. Many different versions have been uploaded to VirusTotal over the years, mainly from Russia, Ukraine, and Uzbekistan. Additionally, sometimes a Telekopye administrator willingly shares the source code, allowing anyone to fork it, as we learned by infiltrating Telekopye groups and analyzing their internal communications. The modified Telekopye source code usually keeps the core unchanged, but adds additional features; therefore we refer to all such variants commonly as Telekopye.

Members of any Telegram group utilizing Telekopye gain access to the bot's UI (see Figure 1). Through it, they are able, in a matter of seconds and without any technical skills, to create everything they need to pull off a scam. By "everything", we mean mainly phishing emails, SMS messages, and web pages. Besides that, Telekopye aids them during the scam as well, as we'll describe later. We have already described, in depth, the basic Telekopye functionality our *first Telekopye blogpost*, in 2023.



💼 Working panel

Select country 3:40 PM

Figure 1. Part of the Telekopye user interface showing the targeted countries. Text was machine translated from Russian to English.

WHO OPERATES TELEKOPYE?

Not all Neanderthals are equal – Telekopye groups have a *clear hierarchy*. At the top of this hierarchy is an Administrator who maintains Telekopye, mainly the phishing domains, email accounts, and such. Aspiring Neanderthals start as regular Workers and, if proven, can be promoted, granting them higher privileges and mainly lowering their fees. Similarly, breaking the rules has consequences – up to and including bannng the Worker. Skilled Workers can offer to help newcomers with onboarding by teaching them.

The groups also manage training materials, implement referral bonuses, and require newcomers to fill out an application form – in short, they operate like a business.

Recruiting new members

Naturally, Workers are the crucial part of the operation, which is why each group wants to have as many as possible. Their numbers in each group vary from tens up to thousands. Neanderthals recruit new members, most commonly on hacking forums. They are very blunt about their operation being about scamming unsuspecting victims. They also usually boast about their best features, as we already mentioned that each groups alters the bot slightly. One such advertisement is illustrated in Figure 2.

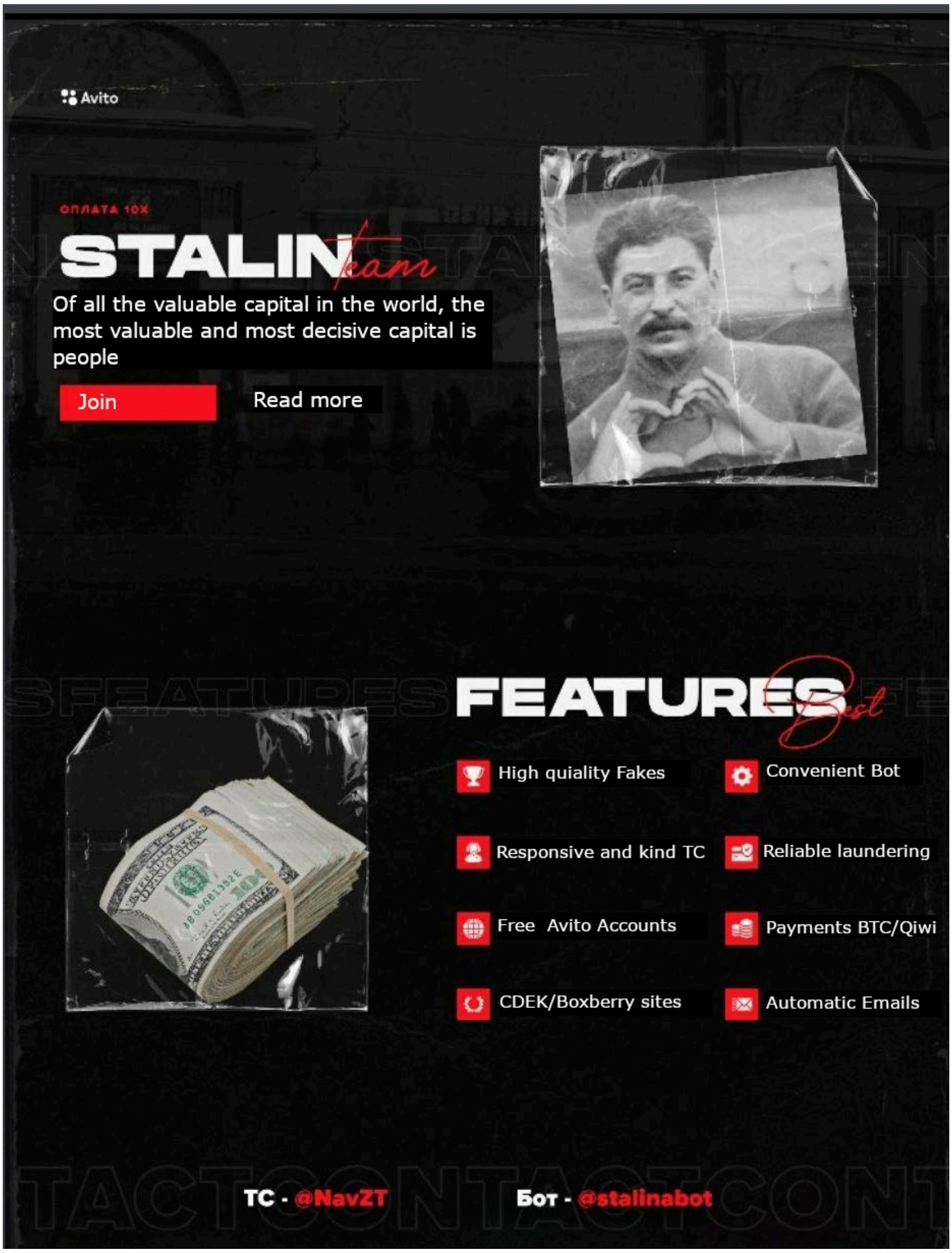
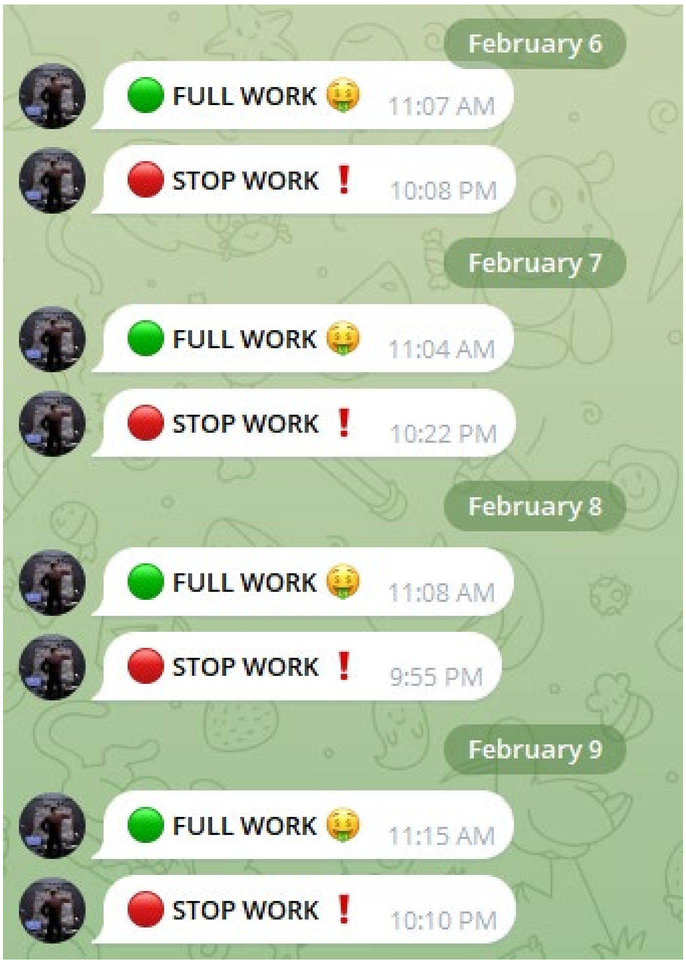


Figure 2. Advertisement of one Telekopye group that calls itself Stalin team. Text was machine translated from Russian to English.

Internal culture

The Telekopye UI is in Russian and the group chat also happens mainly in Russian. This hints that Neanderthals are either Russian nationals or speakers.

One of the rules Neanderthals have to obey is working hours – working outside of the specified timeframe might get them banned. This is probably so that the Administrator can oversee the operation closely. Working hours are announced in the group chat (see Figure 3), although, as the timestamps suggest, not automatically, but manually by the group Administrators.



February 6

🟢 FULL WORK 🤑 11:07 AM

🔴 STOP WORK ❗ 10:08 PM

February 7

🟢 FULL WORK 🤑 11:04 AM

🔴 STOP WORK ❗ 10:22 PM

February 8

🟢 FULL WORK 🤑 11:08 AM

🔴 STOP WORK ❗ 9:55 PM

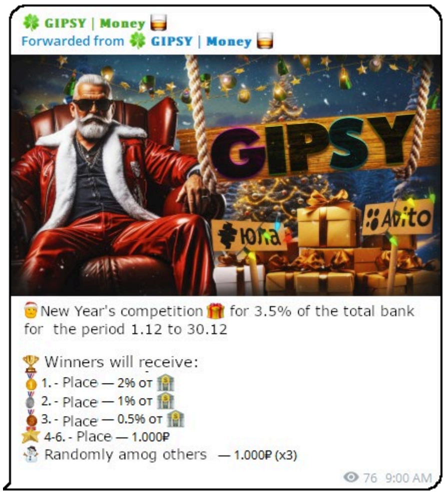
February 9

🟢 FULL WORK 🤑 11:15 AM

🔴 STOP WORK ❗ 10:10 PM

Figure 3. Announcements to start and stop working in a Telekopye group chat, usually made in English

Other than that, the conversations are full of memes and overall very informal content. Occasionally, Administrators post job offers looking for developers and translators. Many groups also regularly organize contests, where they offer extra money to the most productive Worker. Examples of both are shown in Figure 4.

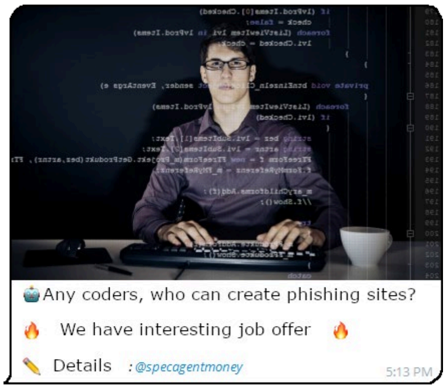


🍀 GIPSY | Money 🥃
Forwarded from 🍀 GIPSY | Money 🥃

🎅New Year's competition 🎁 for 3.5% of the total bank for the period 1.12 to 30.12

🏆 Winners will receive:
🥇 1. - Place — 2% от 🏦
🥈 2. - Place — 1% от 🏦
🥉 3. - Place — 0.5% от 🏦
⭐ 4-6. - Place — 1.000₽
⛄ Randomly amog others — 1.000₽ (x3)

👁 76 9:00 AM



🤖Any coders, who can create phishing sites?

🔥 We have interesting job offer 🔥

✏️ Details : @specagentmoney

5:13 PM

Figure 4. Announcement of a competition for extra money (left) and a job offer posting (right) in Telekopye group chat. Both images had their text machine translated from Russian to English.

Payouts

Interestingly, Neanderthal Workers do not get to keep any stolen sensitive information, nor do they actually steal any money – that is managed by other roles in the organization. When a Worker wants to get paid, he needs to ask Telekopye (this process is automated in some versions when the Neanderthal reaches a certain threshold of successfully pulled scams). The Administrator then needs to approve the request, after which money is transferred to the underling Neanderthal's account (usually a cryptocurency wallet). Additionally, each Telekopye group keeps a transparent chat of all transactions, visible to all members. The process is illustrated in Figure 5.

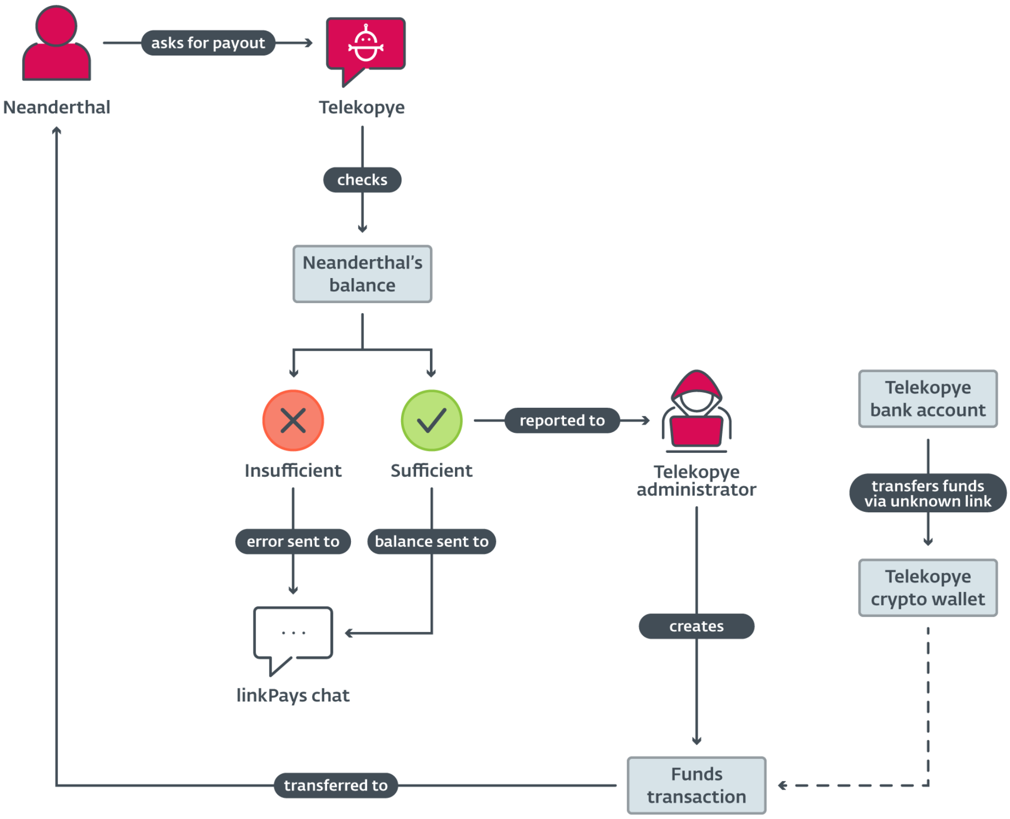


Figure 5. Overview of how Neanderthals are paid by Telekopye Administrators

Operations RIP and VICTORY

In late 2023, Czech and Ukrainian police *arrested* tens of cybercriminals utilizing Telekopye, including the key players, in two joint operations dubbed RIP and VICTORY. Both operations were aimed against a further unspecified number of Telekopye groups. Based on police estimates, the disrupted groups had accumulated at least €5 million since 2021. Besides the obvious success in disrupting such criminal activities, something else was revealed – while many Telekopye groups employ young, non-technical individuals, commonly known as *skiddies*, the groups targeted by these two operations were nothing of that sort.

These Telekopye groups were managed by middle-aged men from Eastern Europe and West and Central Asia who owned dedicated workplaces from where they managed their scamming activities (see Figure 6). They recruited people in difficult life situations, mainly for the money side of the scam – setting up bank and cryptocurrency accounts and sending and extracting stolen money.

These Telekopye groups also posted on job portals promising "easy money", a typical approach to recruiting money mules. Finally, they targeted universities, looking for technically skilled foreign students willing to participate in the more technical parts of the scamming process.

A subset of the perpetrators confessed that they also participated in a scam group similar to the Telekopye ones. That scam group utilized call centers, another common scam technique. The police further learned the recruits in that operation were often stripped of their passports and personal IDs to make quitting such a "job" very difficult. Further, the perpetrators sometimes went so far as to threaten their staff or their family members.

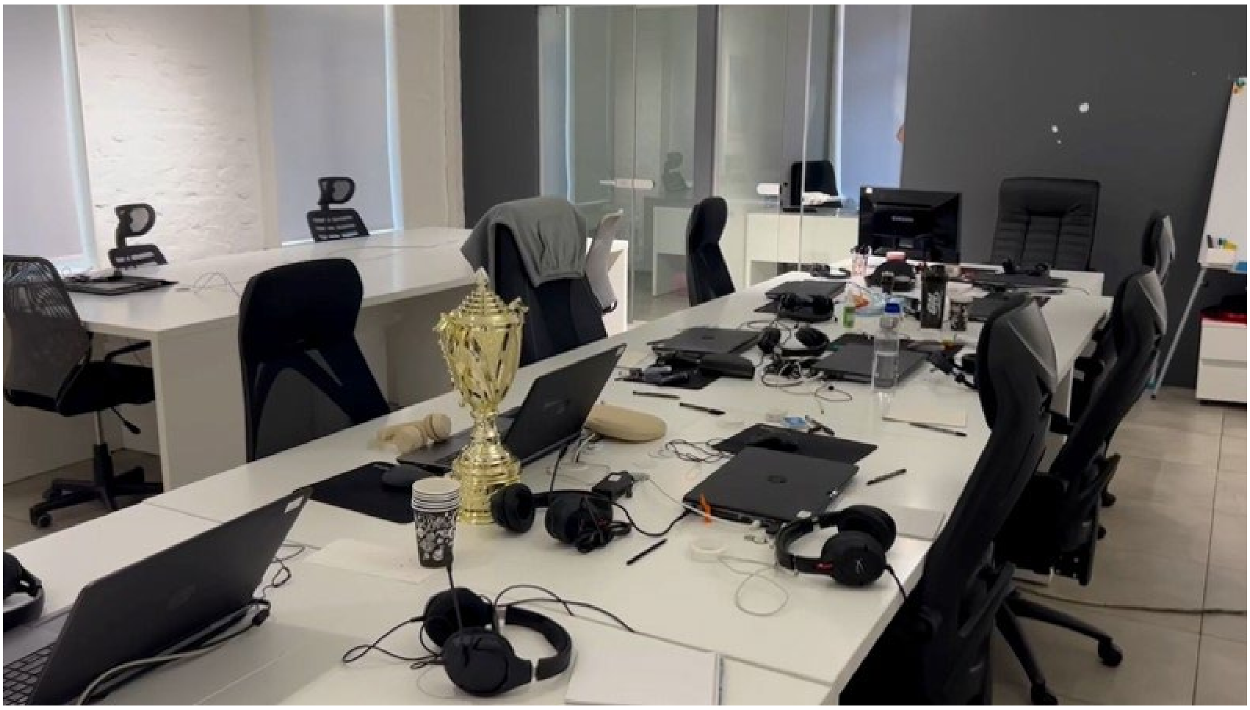


Figure 6. The workplace where a Telekopye group's leadership worked, which was targeted by the RIP and VICTORY operations. Source: Czech police

THE ANATOMY OF THE SCAMS

Neanderthals utilize two main scenarios for targeting online marketplaces – one where they pose as a seller (Seller scenario) and one, much more common, where they pose as a buyer (Buyer scenario). Both scenarios end with the Mammoth entering credit card information or online banking credentials into a phishing web page mimicking a payment gateway. The entered data is then processed by other members of the operation. Let's examine each case.

Seller scenario

In this scenario, the Neanderthal creates a listing for a non-existent item and tries to lure unsuspecting Mammoths into buying it. The Neanderthal persuades the Mammoth to pay online, usually claiming in-person unavailability due to personal or work reasons. The Mammoth then receives a link to a page on a phishing website. That page masquerades as an item order summary, with a `Next` button that leads to a web page mimicking a payment gateway.

The Seller scenario is easier to manage for Neanderthals, but they need to wait for Mammoths to show interest. Also, the Neanderthal's account will probably be suspended after the first scam is pulled.

Buyer scenario

In this scenario, the Neanderthal looks up "suitable" items that Mammoths are selling (the process of deciding what item is "suitable" is quite complex and we described it in our *second Telekopye blogpost*). The Neanderthal then contacts the Mammoth, feigning interest. More skilled Neanderthals will engage in a short conversation first, while most of them will just claim right away that they are interested and ask to go to payment straight away. Since the Mammoths are *selling* and not *buying*, how are they persuaded to give up their financial information?

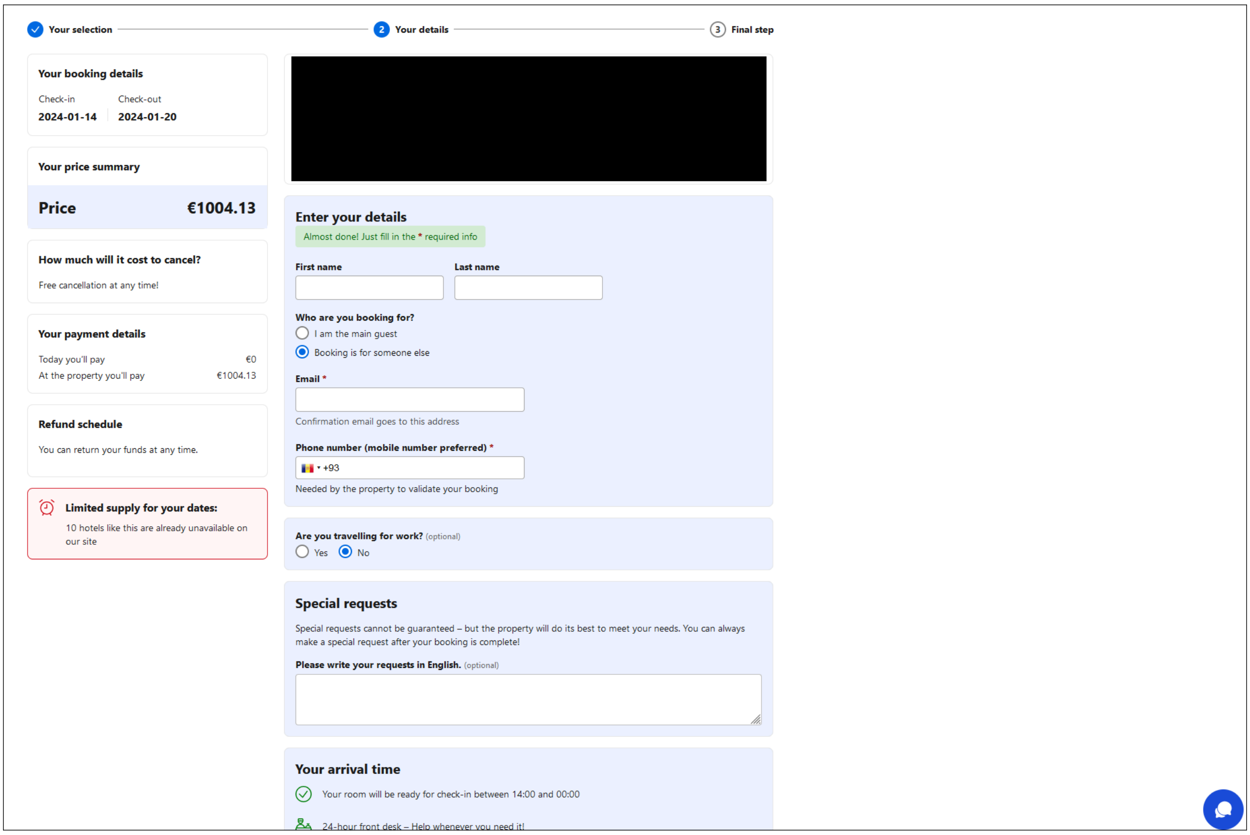
The first tactic Neanderthals use is to claim that they already paid "to the service" and that the Mammoth needs to enter their information to receive the money "from the service". A link to a phishing website with a button to do so follows.

The other tactic is to abuse a well-known courier service. Neanderthals claim they already paid for the courier to come and pick up the package and the Mammoth just needs to pay an insurance fee. Both tactics end with the Mammoth receiving a link to a phishing website.

Expanding – accommodation services

In the past, Neanderthals experimented with a *scam scenario* targeting the real estate market. They looked up a real apartment for rent, then contacted the renter and obtained as much details as possible. Next, they offered to rent out the same apartment on a different website, but with a lower price. When a Mammoth was interested in renting, they requested a reservation fee and that way stole the money.

However, the scenario likely proved ineffective or too dangerous and Neanderthals chose a different strategy – targeting popular online platforms for hotel and apartment reservations. In this scenario, they send an email to a user of such a platform, informing the target that there has been an issue with their payment and they need to fix it. The email, unsurprisingly, contains a link to a well-crafted, legitimate-looking web page (an example is shown in Figure 7).



✓ Your selection — 2 Your details — 3 Final step

Your booking details

Check-in	Check-out
2024-01-14	2024-01-20

Your price summary

Price **€1004.13**

How much will it cost to cancel?

Free cancellation at any time!

Your payment details

Today you'll pay	€0
At the property you'll pay	€1004.13

Refund schedule

You can return your funds at any time.

Limited supply for your dates:

10 hotels like this are already unavailable on our site

[redacted]

Enter your details

Almost done! Just fill in the * required info

First name **Last name**

Who are you booking for?

○ I am the main guest

● Booking is for someone else

Email *

Confirmation email goes to this address

Phone number (mobile number preferred) *

+93

Needed by the property to validate your booking

Are you travelling for work? (optional)

○ Yes ● No

Special requests

Special requests cannot be guaranteed – but the property will do its best to meet your needs. You can always make a special request after your booking is complete!

Please write your requests in English. (optional)

Your arrival time

✓ Your room will be ready for check-in between 14:00 and 00:00

24-hour front desk – Help whenever you need it!

Figure 7. Example of a fake Booking.com registration form created by Telekopye

While some personal information is requested (name, email, phone), others are prefilled, such as the check-in and check-out dates, price, and the details of the destination. But why would a random user pay for a vacation he has no idea of purchasing? Because, in this scenario, Neanderthals do not target random users. They utilize compromised accounts of legitimate hotels and renters on the platforms. Using those, they obtain a list of users who recently booked a stay and didn't pay yet or paid very recently and target them, leading to a much higher expected success rate.

ADVANCED, CUSTOMIZED FEATURES

As already mentioned, different groups implement their own custom features. Let's look more closely at some of the convenient modifications Neanderthals have come up with over the years while highlighting their importance in the operation.

Speeding up creation process

The typical process of creating scam materials for Buyer scenario using Telekopye goes like this:

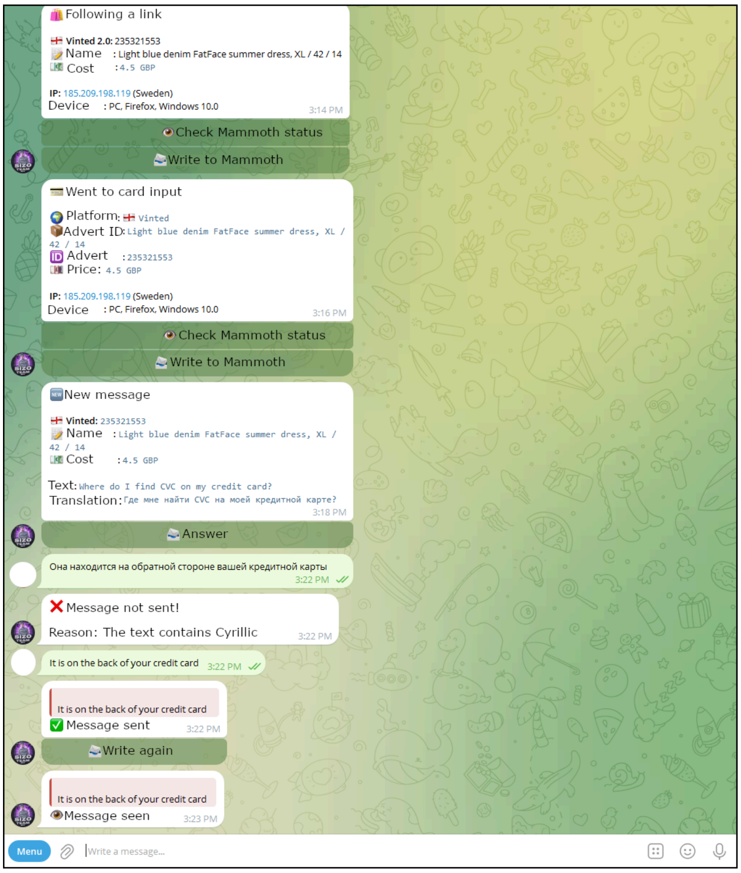
1. The Neanderthal selects the targeted country and service or platform.
2. The Neanderthal answers a questionnaire. Questions aim mainly at the Mammoth's name, address and other personal information known initially, and the name, price, and image of the goods.
3. Telekopye takes the Neanderthal's answers and uses them to generate a legitimate-looking phishing web page.

At that point, the Neanderthal has everything necessary for performing the scam. The communication with the Mammoth is up to them, though Telekopye assists with that too, as we'll see shortly. Regardless, even answering 10 to 15 questions seems like too much work, so the Neanderthals came up with a shortcut. Instead of answering questions, they implemented web scrapers for popular targeted platforms. With these, only the URL to the product is required. Telekopye then parses the web page and extracts all necessary information automatically. This provides a significant speedup.

Chatbot

While a few Russian online marketplaces, such as Youla and Avito, are targeted by Neanderthals, they mostly focus on Europe and North America. This obviously brings up the issue of a language barrier. Just like scam call centers have their scripts, Neanderthals have a huge collection of predefined answers to commonly asked questions, translated into various languages and kept as part of internal documentation. Their translation has been perfected over the years.

Neanderthals usually try to quickly direct the Mammoth to the phishing website using those predefined phrases. Once there, the Mammoth is greeted with a legitimate-looking web page with an important feature – a chatbot in the lower right corner. Any message the Mammoth enters into the chat gets immediately passed to the Neanderthal's Telegram chat. And not only that, it also gets automatically translated as well. Automatic translation of Neanderthals' messages is not supported – Neanderthals usually use DeepL to translate their messages to the Mammoth manually. Figure 8 shows how such an interaction looks from both the Mammoth's and Neanderthal's points of view. Notice that when attempting to send a response in Cyrillic, Telekopye shows a warning that Cyrillic letters are present and does not forward that message to the Mammoth. Additionally, you can see that Telekopye also notifies the Neanderthal that the Mammoth visited the link and that he got to the stage of entering card details.



🛍 Following a link

Vinted 2.0: 235321553
📝 Name : Light blue denim FatFace summer dress, XL / 42 / 14
💵 Cost : 4.5 GBP

IP: 185.209.198.119 (Sweden)
Device : PC, Firefox, Windows 10.0 3:14 PM

💳 Went to card input

🌍 Platform: Vinted
📦 Advert ID: Light blue denim FatFace summer dress, XL / 42 / 14
🆔 Advert : 235321553
💷 Price: 4.5 GBP

IP: 185.209.198.119 (Sweden)
Device : PC, Firefox, Windows 10.0 3:16 PM

🆕 New message

Vinted: 235321553
📝 Name : Light blue denim FatFace summer dress, XL / 42 / 14
💵 Cost : 4.5 GBP

Text: Where do I find CVC on my credit card?
Translation: Где мне найти CVC на моей кредитной карте? 3:18 PM

Она находится на обратной стороне вашей кредитной карты 3:22 PM ✓✓

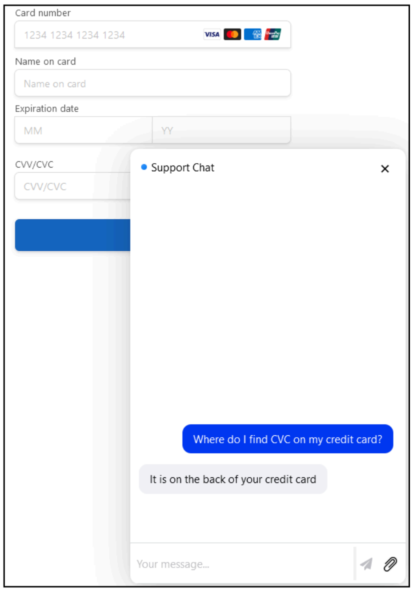
❌ Message not sent!

Reason: The text contains Cyrillic 3:22 PM

It is on the back of your credit card 3:22 PM ✓✓

It is on the back of your credit card
✅ Message sent 3:22 PM

It is on the back of your credit card
👁 Message seen 3:23 PM



Where do I find CVC on my credit card?

It is on the back of your credit card

Figure 8. Chatbot feature example from Neanderthal's (left) and Mammoth's (right) point of view. Telekopye messages on the left side were machine translated from Russian to English.

This is an important feature. All of the translation happens automatically and fast compared to manual translation of every message the Mammoth writes. And since chatbots in general are a popular feature and many users are familiar with them, Neanderthals expect them to use it and if they pose convincingly enough, it may be the final nail in the Mammoth's coffin.

Phishing web page protection

The vast majority of the phishing websites are serviced by Cloudflare, relying on the added protection, mainly against crawlers and automatic analysis. To our surprise, some of the Telekopye phishing websites also come with DDoS protection included. Protecting against too many Mammoths at once does not really make sense, as even with all the optimizations, the scams are still, at least partially, manually managed. Similarly, law enforcement operations would likely choose more effective tactics than DDoS. We later found the real reason hidden inside the Neanderthals' knowledge base – protecting against competitor groups.

As you can imagine, all Telekopye groups are rivals. They constantly try to steal other groups' Workers and shame each other. Occasionally, they also launch a DDoS attack on their competitors as means to demonstrate strength and to disrupt their operation for a short period of time. Figure 9 shows such protection in place.

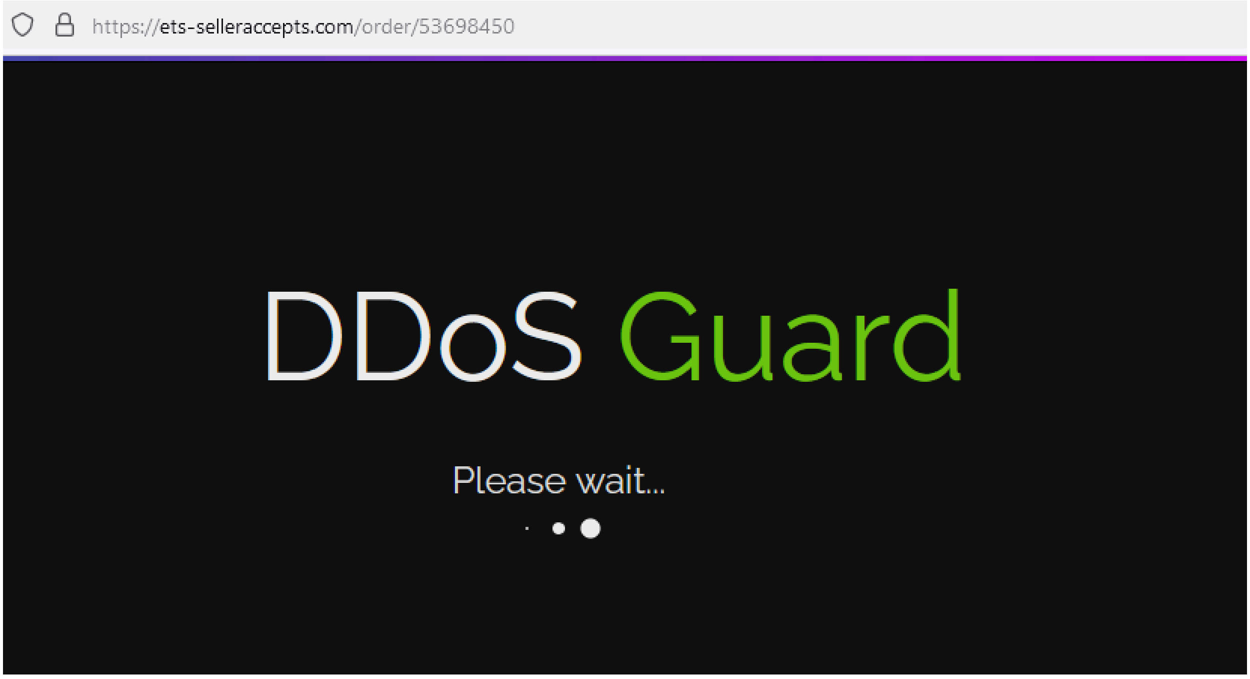


Figure 9. DDoS protection of a phishing domain

HOW TO STAY PROTECTED

The best way to stay protected against Telekopye-driven scams is definitely awareness. In this section, we will walk you through the stages of the scam with focus on what to pay attention to in order to evade Neanderthals' spears.

You should consider using an antimalware solution on your device. If the Neanderthal manages to lure you to the point where you visit the phishing website, the solution may recognize its maliciousness and warn you.

One unintended issue of online marketplaces is that the sales happen very conveniently and therefore, after some time, we get too comfortable with the process and lower our guards. Never try to rush with sales on these platforms. Take your time, think about the process, and be extra careful if anything makes you so much as knit your brow.

On the platform

With the improvements in translators and further integration of LLMs, incorrect grammar is becoming less and less of an issue. Keep that in mind when talking to any potential buyer or seller and focus rather on the conversation itself. Be especially careful if you are new on the platform.

Overly eager buyers and sellers should raise some concerns. Always verify the person you are talking with, mainly their history on the platform, age of their account, rating, and location. A location too far away (especially in smaller countries), a fresh account with no history, or a bad rating are good indicators of a potential scammer. Remember that Neanderthals also use compromised accounts, in which case these indicators may reveal nothing.

Always insist on in-person exchange of goods and money whenever possible. If that is not possible and you are a buyer, don’t pay up front. Reliable delivery services offer the option to pay on delivery, which is ideal for this case. If you are a seller, always manage delivery options yourself and don’t agree to those offered (often too enthusiastically) by the buyer. If they claim they already paid “to the platform”, either don’t believe them or verify that with official customer support of the platform.

Outside the platform

If a potential Neanderthal suggests moving the communication elsewhere for whatever reason, do not do it. There is a reason why these platforms prefer their own chats and that is because they can, to an extent, warn you of suspicious behavior – for example, sending URLs is very uncommon there, so it may immediately raise some red flags.

Some online marketplaces, mostly for legacy reasons, rely on communication outside of the platform. If that is the case, be extra careful. If you feel like something is not right, always double check with the platform.

On the phishing website

If you get to a point where you visit the link provided by a Neanderthal, be sure to check it carefully, mainly:

- the URL – you can, for example, search for the URL using a search engine, which will usually quickly uncover the malicious intent,
- the content – any visual issues, spelling errors, unusual information being requested should raise concerns, and
- the certificate – pay attention to both the issuer and the subject and the validity timestamps.

If you submitted your data

If you indeed submitted your data and realize later that it may have been a mistake, waste no time and contact your bank. Block your credit or debit card and consult with your bank on additional steps. If financial loss has happened, reach out to law enforcement.

Similarly, if you submitted your email address or phone number, be extra careful about the messages you receive, especially in a short period of time. Even if you didn’t lose any money, Neanderthals may still try to use this information to further scam you in various ways.

CONCLUSION

We have introduced Telekopye, a versatile Swiss Army knife for turning online marketplace scams into an organized illicit business. We have demonstrated it is widespread and how dangerously easy to use the bot is. We have further focused on some of its more advanced features that offer powerful capabilities to the Neanderthals.

Our research gave us a unique peek behind the curtain of these scams. We were able to understand the technical means behind why so many such scams are happening daily, the true business side of Telekopye groups, and even learn about Neanderthals themselves.

We have covered the common scenarios Neanderthals use to target users of online marketplaces and described their newest approach of targeting accommodation offering platforms. Understanding the scenarios is crucial for realizing that the other party may have malicious intent.

With the popularity of online marketplaces, sales happening on these platforms will only grow. It is unlikely that such scams will disappear in the near future, especially since they are profitable for the Neanderthals. However, that does not mean we are helpless. During our research, we communicated with several platforms targeted by Telekopye and they are very aware of these scams and their defenses are more capable than it may seem. Additionally, awareness is absolutely key. We have shown that these scams are effective and the cybercriminals behind them continuously improve their tactics and adapt to new trends. Anyone can fall victim, if suitably targeted. In our paper, we give examples of what to pay attention to in each stage of the scam. Spreading awareness and realizing the specific red flags to pay attention to is the best way to avoid Neanderthals' spears.

IOCS

SHA-1	Filename	Detection	Description
E815A879F7F30FB492D4043F0F8C67584B869F32	scam.php	PHP/HackTool.Telekopye.B	Telekopye bot.
378699D285325E905375AF33FDEB3276D479A0E2	scam.php	PHP/HackTool.Telekopye.B	Telekopye bot.
242CE4AF01E24DB054077BCE3C86494D0284B781	123.php	PHP/HackTool.Telekopye.A	Telekopye bot.
9D1EE6043A8B6D81C328C3B84C94D7DCB8611262	mell.php	PHP/HackTool.Telekopye.B	Telekopye bot.
B0189F20983A891D0B9BEA2F77B64CC5A15E364B	neddoss.php	PHP/HackTool.Telekopye.A	Telekopye bot.
E39A30AD22C327BBBD2B02D73B1BC8CDD3E999EA	nscode.php	PHP/HackTool.Telekopye.A	Telekopye bot.
285E0573EF667C6FB7AEB1608BA1AF9E2C86B452	tinkoff.php	PHP/HackTool.Telekopye.A	Telekopye bot.

IP	Domain	Hosting provider	First seen	Details
N/A	3-dsecurepay[.]com	Cloudflare, Inc.	2024-05-30	Telekopye phishing domain.
N/A	approveine[.]com	Cloudflare, Inc.	2024-06-28	Telekopye phishing domain.
N/A	audittravelerbookdetails[.]com	Cloudflare, Inc.	2024-06-01	Telekopye phishing domain.
N/A	btsdostavka-uz[.]ru	TIMEWEB-RU	2024-01-02	Telekopye phishing domain.
N/A	burdchoureserdoc[.]com	Cloudflare, Inc.	2024-05-31	Telekopye phishing domain.
N/A	check-629807-id[.]top	Cloudflare, Inc.	2024-05-30	Telekopye phishing domain.
N/A	contact-click2399[.]com	Cloudflare, Inc.	2024-05-26	Telekopye phishing domain.
N/A	contact-click7773[.]com	Cloudflare, Inc.	2024-05-30	Telekopye phishing domain.
N/A	get3ds-safe[.]info	Cloudflare, Inc.	2024-05-31	Telekopye phishing domain.
N/A	hostelguest[.]com	Cloudflare, Inc.	2024-05-30	Telekopye phishing domain.
N/A	order-9362[.]click	Cloudflare, Inc.	2024-05-29	Telekopye phishing domain.
N/A	shiptakes[.]info	Cloudflare, Inc.	2024-05-29	Telekopye phishing domain.
N/A	quickroombook[.]com	Cloudflare, Inc.	2024-06-02	Telekopye phishing domain.
N/A	validation-confi[.]info	Cloudflare, Inc.	2024-05-29	Telekopye phishing domain.

MITRE ATT&CK TECHNIQUES

Tactic	ID	Name	Description
Reconnaissance	T1589	Gather Victim Identity Information	Telekopye is used to gather debit/credit card details, phone numbers, emails, etc. via phishing web pages.
Resource Development	T1583.001	Acquire Infrastructure: Domains	Telekopye operators register their own domains.
	T1585	Establish Accounts	Telekopye operators establish accounts at online marketplaces.
	T1585.002	Establish Accounts: Email Accounts	Telekopye operators set up email addresses associated with the domains they register.
	T1586.002	Compromise Accounts: Email Accounts	Telekopye operators use compromised email accounts to increase their stealthiness.
	T1587.001	Develop Capabilities: Malware	Telekopye is custom malware.
	T1588.002	Obtain Capabilities: Tool	Telekopye operators use additional bots to launder money, scrape market research, and implement DDOS protection.
Initial Access	T1566.002	Phishing: Spearphishing Link	Telekopye sends emails or SMS messages that contain links to phishing websites.
Collection	T1056.003	Input Capture: Web Portal Capture	Web pages created by Telekopye capture sensitive information and report it to the operators.