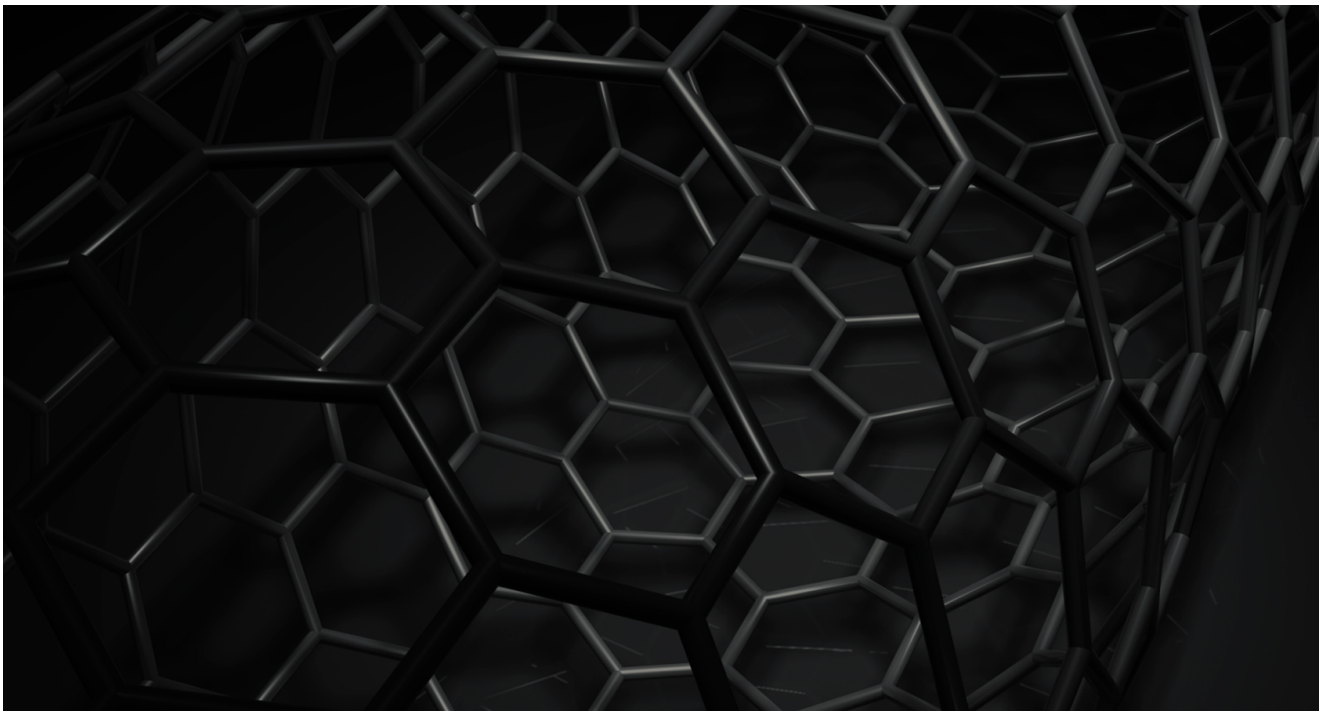
The Fraud Family

blog.group-ib.com/fraud_family_nl/



22.07.2021

Fraud-as-a-Service operation targeting Dutch residents

Roberto Martinez

Senior Threat Intelligence Analyst at Group-IB Europe

Anton Ushakov

Deputy Head of the High-Tech Crime Investigation Department at Group-IB Europe

Introduction

Since the beginning of 2020, Dutch and Belgian residents have been increasingly targeted by financially motivated cybercriminals looking to obtain access to their bank accounts. In many strikingly similar cases, fraudsters reach out to victims via email, SMS, or WhatsApp messages to deliver fake notifications containing malicious links pointing to a phishing site. The phishing pages, detected by Group-IB Threat Intelligence & Attribution system, are almost identical and disguised to look like legitimate banking websites of the biggest local financial organizations with the goal of tricking unsuspecting victims into providing their personal and banking information.

Having analyzed the technical infrastructure and phishing templates used in these fraudulent campaigns, Group-IB Threat Intelligence and Cyber Investigations teams uncovered a massive Fraud-as-a-Service operation. Our researchers identified a Dutch-speaking criminal syndicate, codenamed **Fraud Family** by Group-IB, which develops, sells and rents sophisticated phishing frameworks to other cybercriminals targeting users mainly in the **Netherlands and Belgium**. The phishing frameworks allow attackers with minimal skills to optimize the creation and design of phishing campaigns to carry out massive fraudulent operations all the while bypassing 2FA.

Fraud Family advertises their services and interacts with fellow cybercriminals on Telegram messenger. The criminal syndicate is likely to be active since at least 2020. However, phishing kits similar to those advertised by the group were already used to target Dutch residents as early as 2018. Group-IB shared its findings with the Dutch Police immediately

upon discovery and notified the organizations whose names are being abused by fraudsters. **The probe initiated as a consequence resulted in the arrest of two individuals by the Dutch Police.** The arrested suspects, a 24-year-old man and a 15-year-old man, are thought to be the developer and seller of the Fraud Family phishing framework. The 24-year-old suspect will be arraigned before the examining magistrate in Rotterdam on Friday, July 23, while his 15-year-old accomplice has since been released pending further investigation.

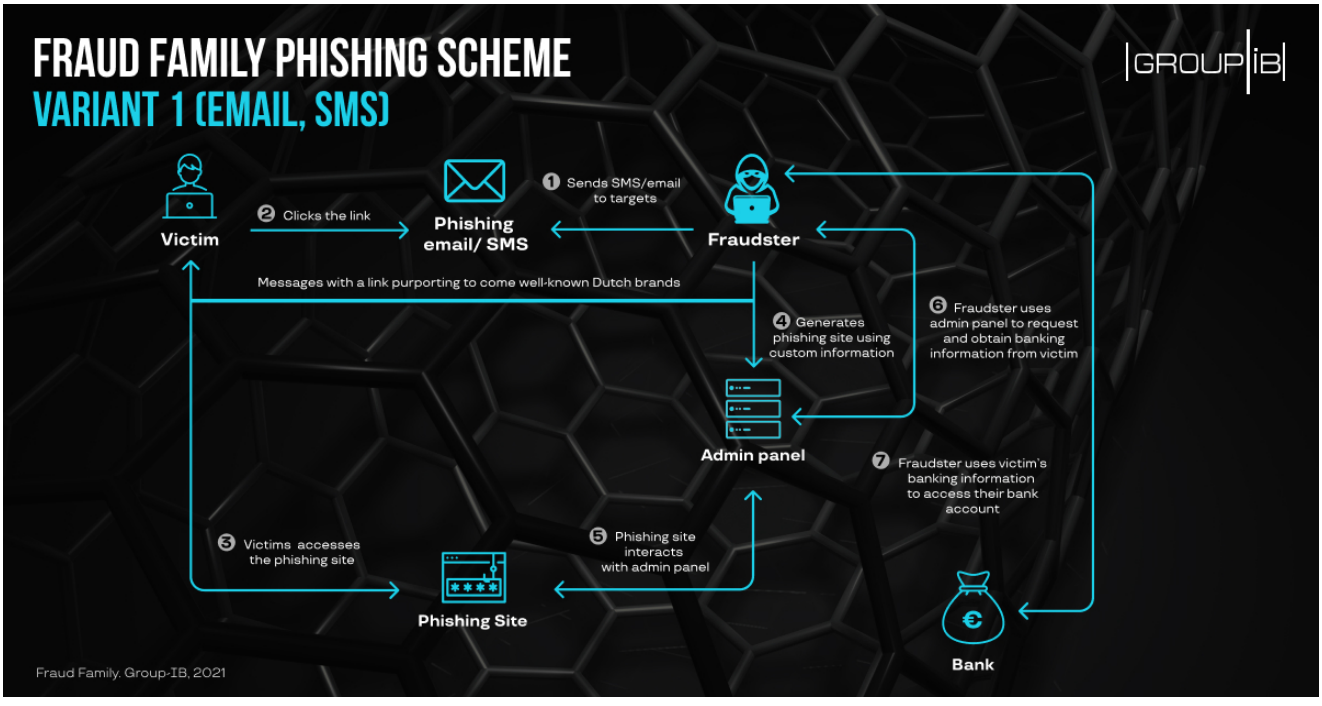
The blog post analyzes the methods and techniques used by Fraud Family's shady customers, Fraud Family's technical infrastructure, and their phishing panels. Group-IB researchers also described how Fraud Family attracts customers and interacts with fellow criminals. The post provides comprehensive recommendations to regular users on how not to fall prey to this type of attack.

Fraudulent journey

A typical attack of fraudsters who use Fraud Family's phishing infrastructure starts with an email, SMS, or WhatsApp message impersonating a real company. The examples below are fraudsters' emails and SMS masked as legitimate messages from a local company that connects home seekers with the housing supply.

Such messages can be both targeted or sent out to multiple contacts at once. The victims' contact details are usually obtained from leaked databases or from other criminals that specialize in providing compromised personal information for social engineering attacks.

The tactic of using well-known brands allows fraudsters to gain users' immediate trust. These fake notifications contain malicious links to adversary-controlled payment info-stealing phishing websites.



Geachte heer/mevrouw,

U heeft een inschrijving bij

Over 2 weken verloopt uw inschrijving.
Uw inschrijving verlengen wij met een jaar als u de verlenginskosten van €8,00 betaalt.
U kunt betalen via
Via de onderstaande link word u automatisch doorverwezen naar onze betaalpagina.

verlengingskosten

Uw factuurnummer is

Machtiging afgeven.

Wilt u betalen via een doorlopende machtiging?
dit kan, nadat u dit jaar nog via betaald heeft.
U kunt na de betaling bij overzicht van mijn gegevens uw betaalwijze veranderen.
Volgend jaar zullen wij dan de verlengingskosten van uw rekening incasseren.
Ook hiervan krijgt u via e-mail een bericht.
Meer informatie over betalen van de verlengingskosten vindt u op onze website.

Uitschrijven.

Als u niet binnen 2 weken betaalt, schrijven wij u uit.
Uw opgebouwde inschrijfduur en eventuele reacties vervallen dan.

Met vriendelijke groet,

Manager Klantcontactcentrum

Figure 1 *Phishing email impersonating a local company company that connects home seekers with the housing supply*
Source: fraudehelpdesk.nl

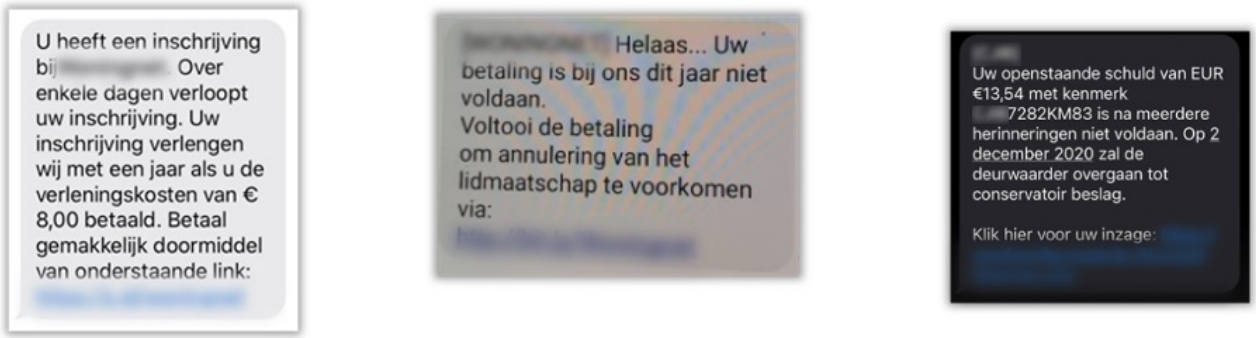


Figure 2 SMS messages containing malicious links
Source: fraudehelpdesk.nl

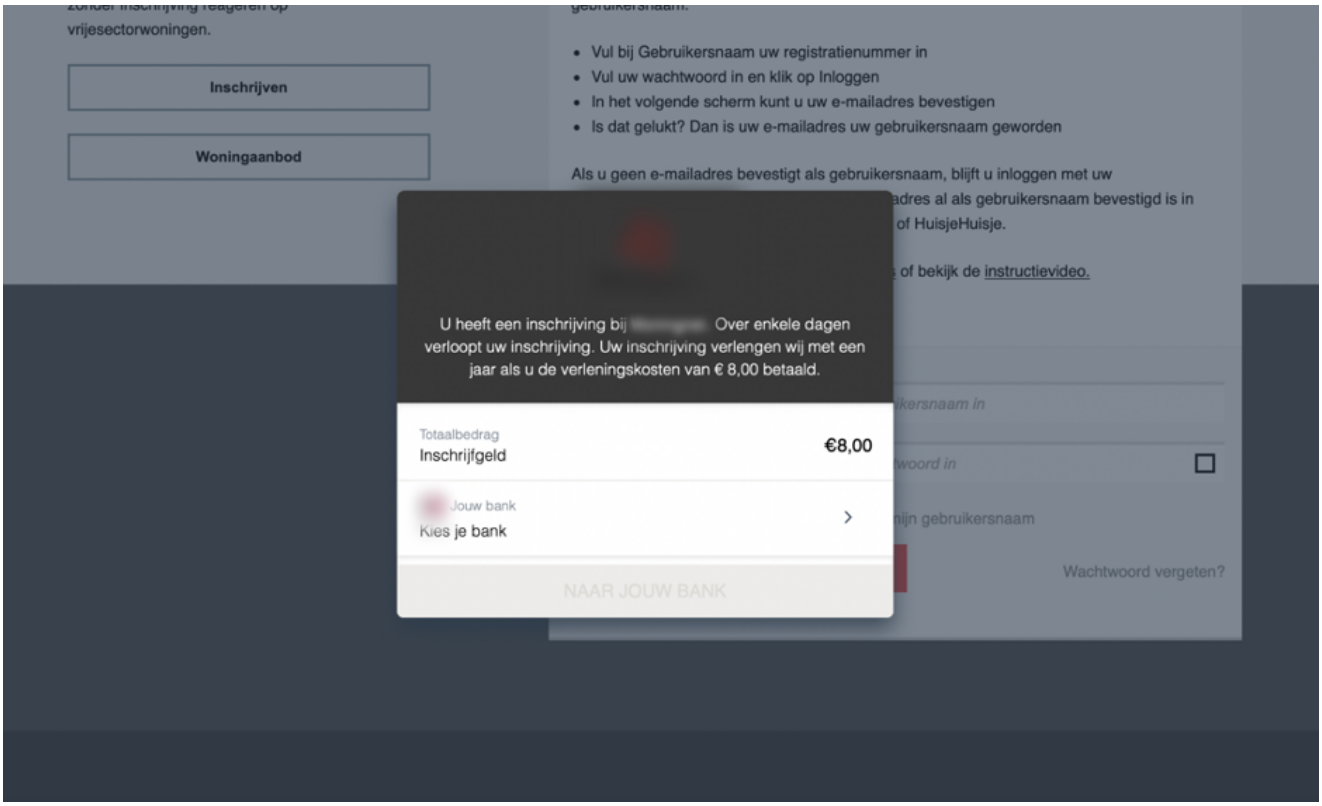
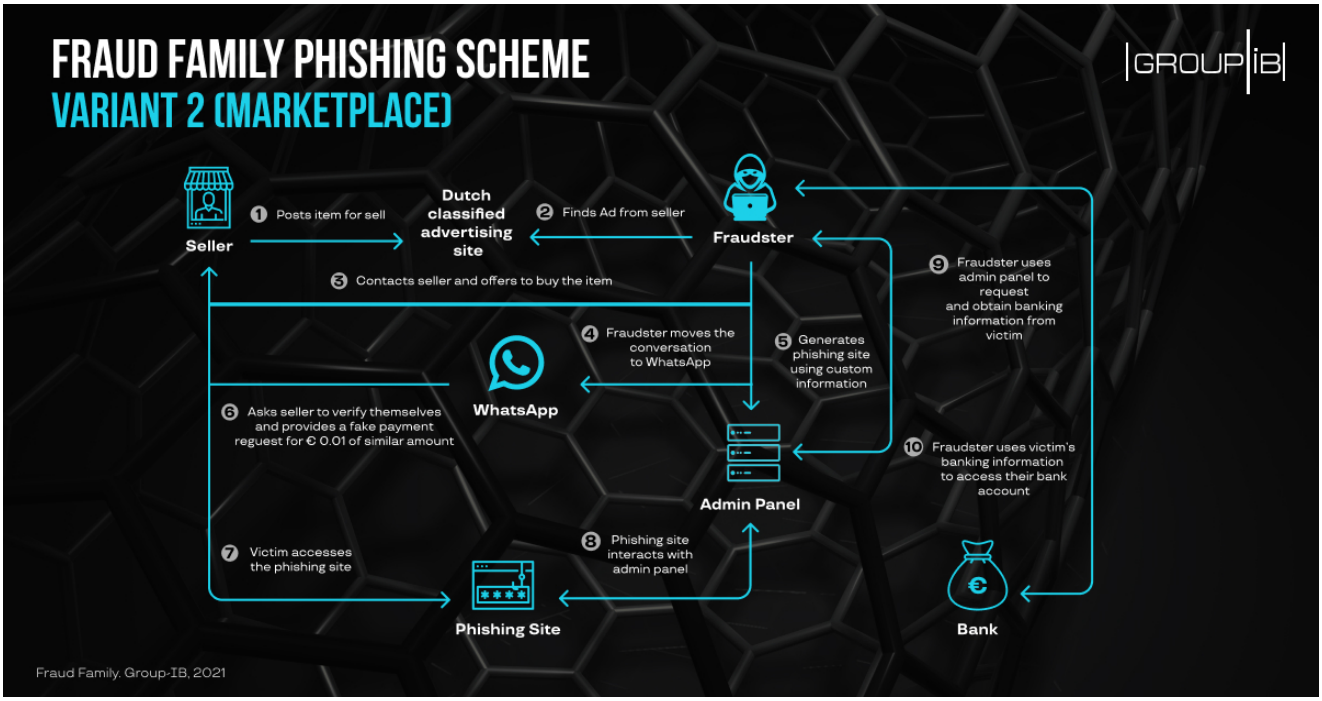


Figure 3 Phishing site impersonating a local company that connects home seekers with the housing supply

Another tactic that we observed recently is when fraudsters contact a seller on a Dutch classified advertising platform pretending to be a buyer. The miscreants first move the conversation to a third-party messenger, WhatsApp in this case, and then proceed to ask the seller to make a small payment using an e-commerce payment system used in the Netherlands, to "verify the seller is not a scammer". The real scammer provides a payment link that is none other than a phishing site. This method was well documented by Opgelicht?!



The phishing website (Fig.4) impersonates a well-known marketplace first, then pretends to use Dutch e-commerce payment system to handle the payment and finally lands on the fake banks' pages. After the seller, now a victim, clicks on the phishing site they get to select which bank they would like to use to send the "small payment".

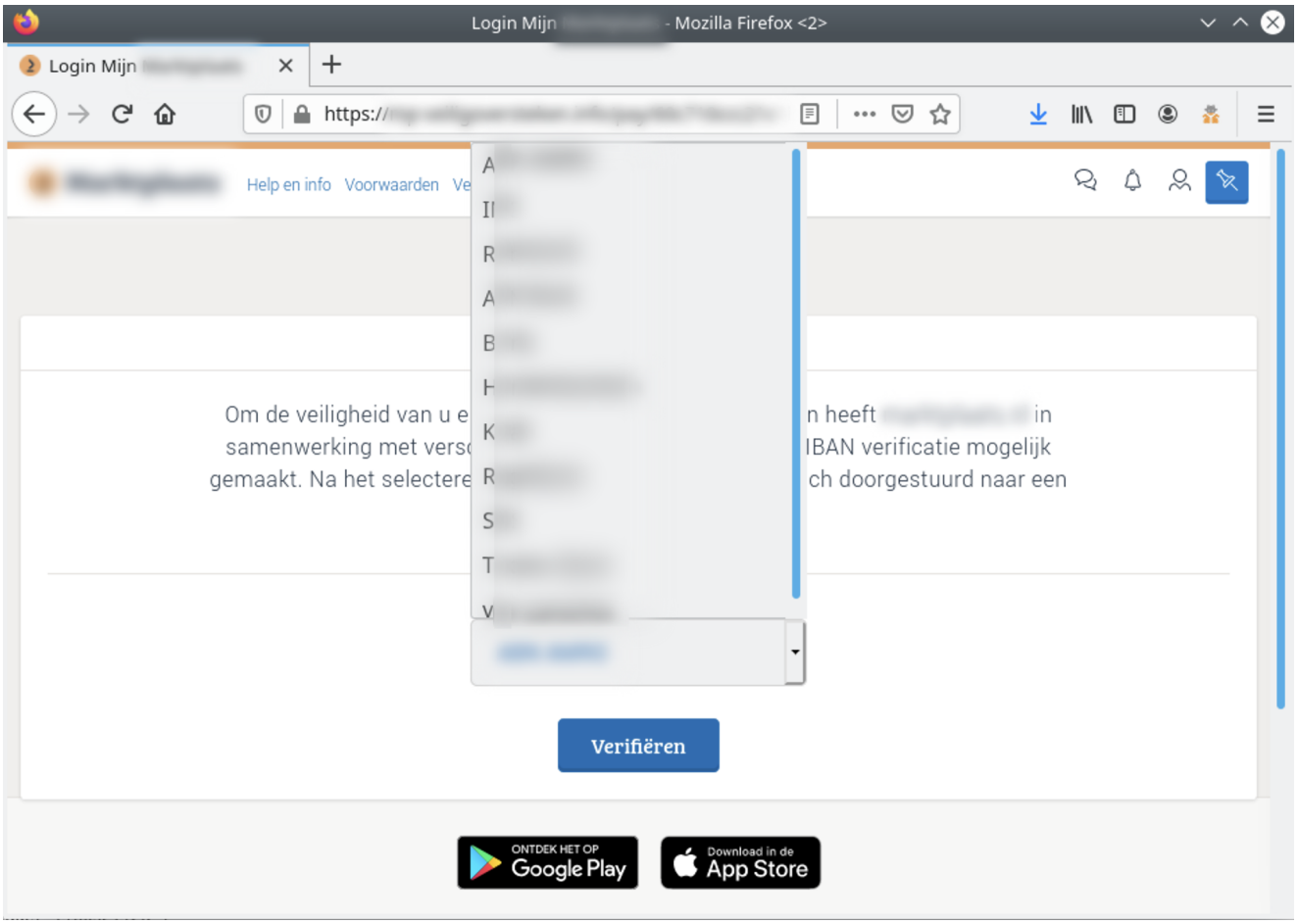


Figure 4 *Phishing site using Dutch online Marketplace* lure

These phishing websites offer a high level of personalization. Once the victim selects a bank from the list, which includes all known local financial organizations, a very convincing online banking interface will be shown asking for their banking credentials: username and password or the bank card number, depending on what they need to access a particular bank account.

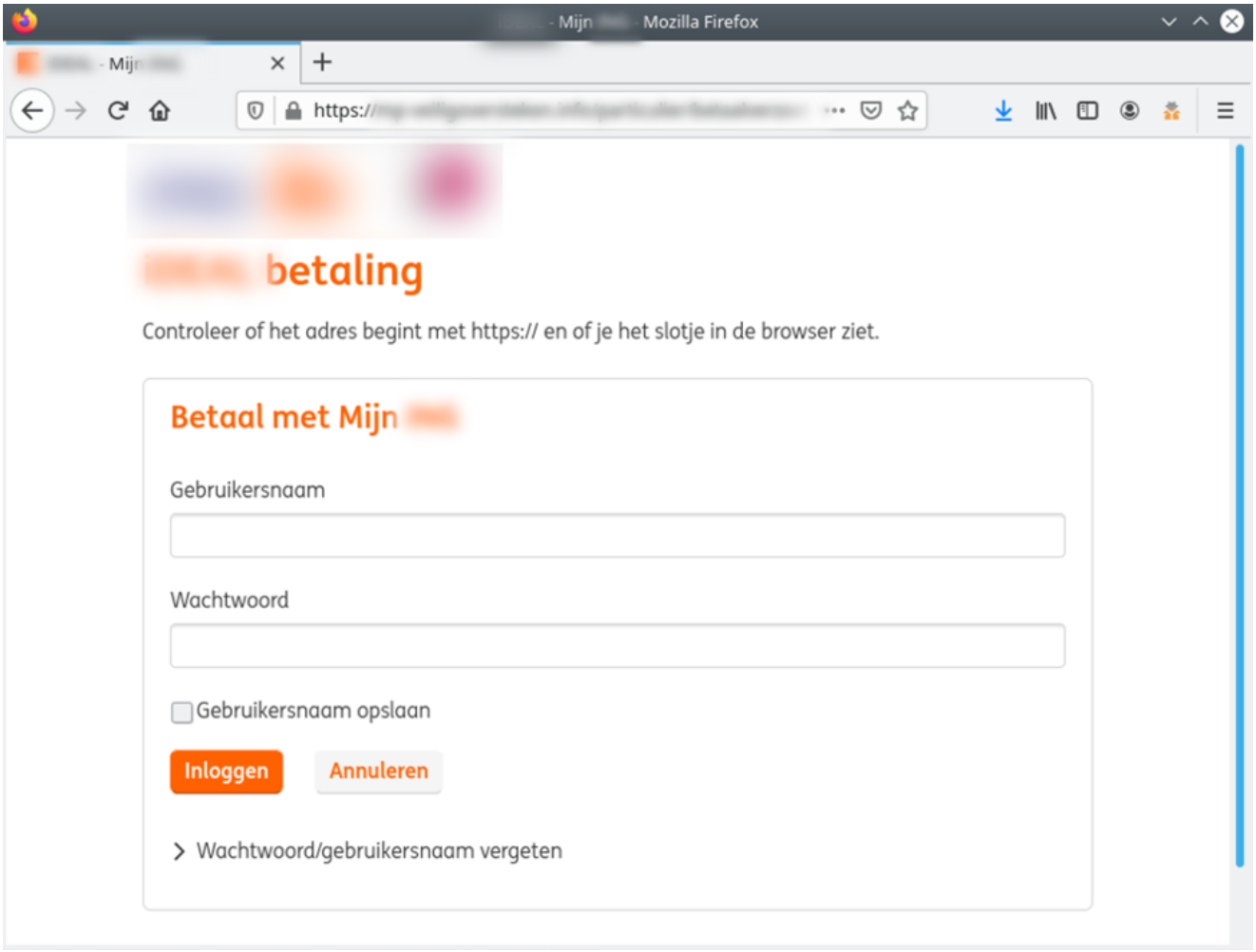


Figure 5 *Phishing website impersonating login interface of a Dutch bank*

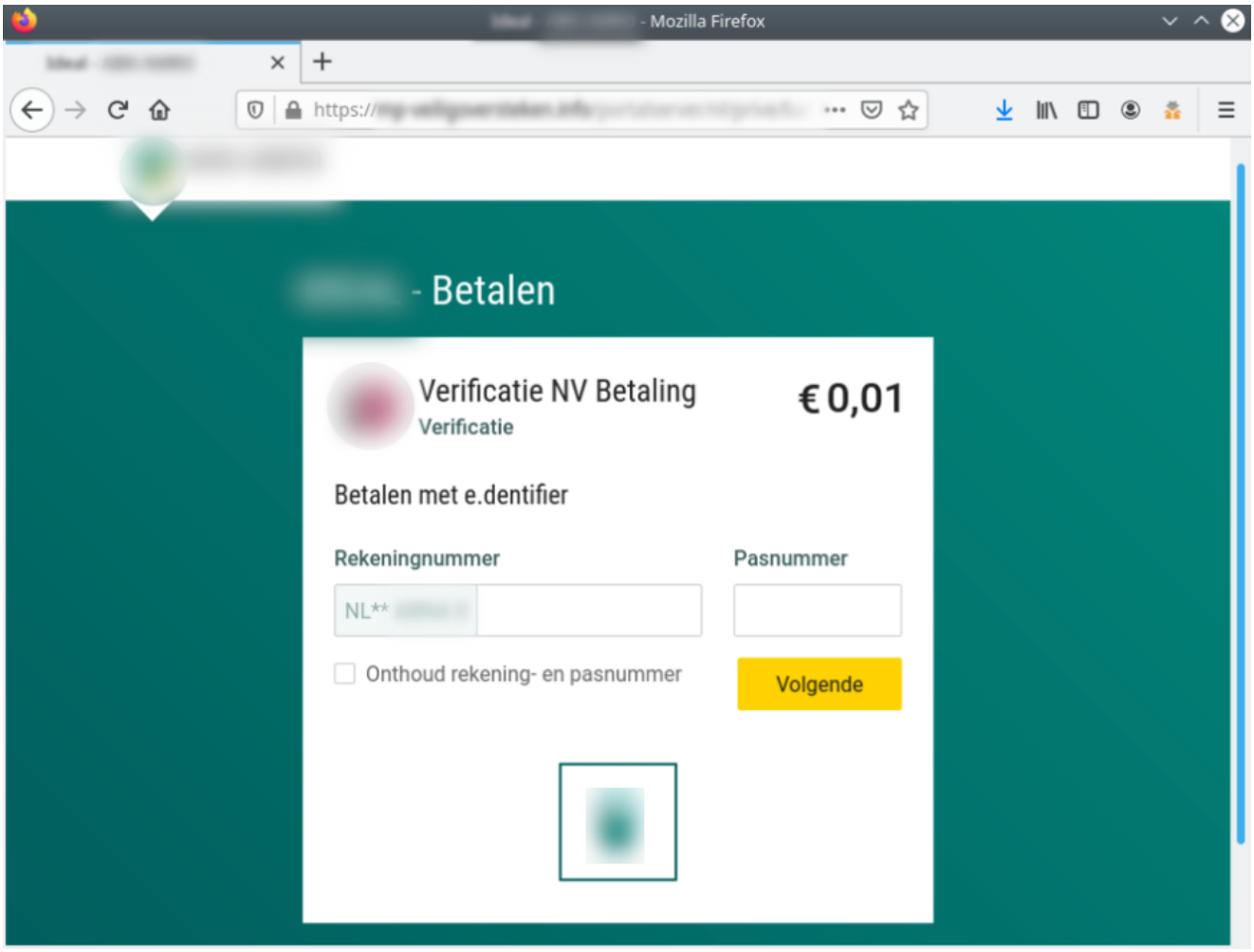


Figure 6 *Phishing website impersonating login interface of a Dutch bank*

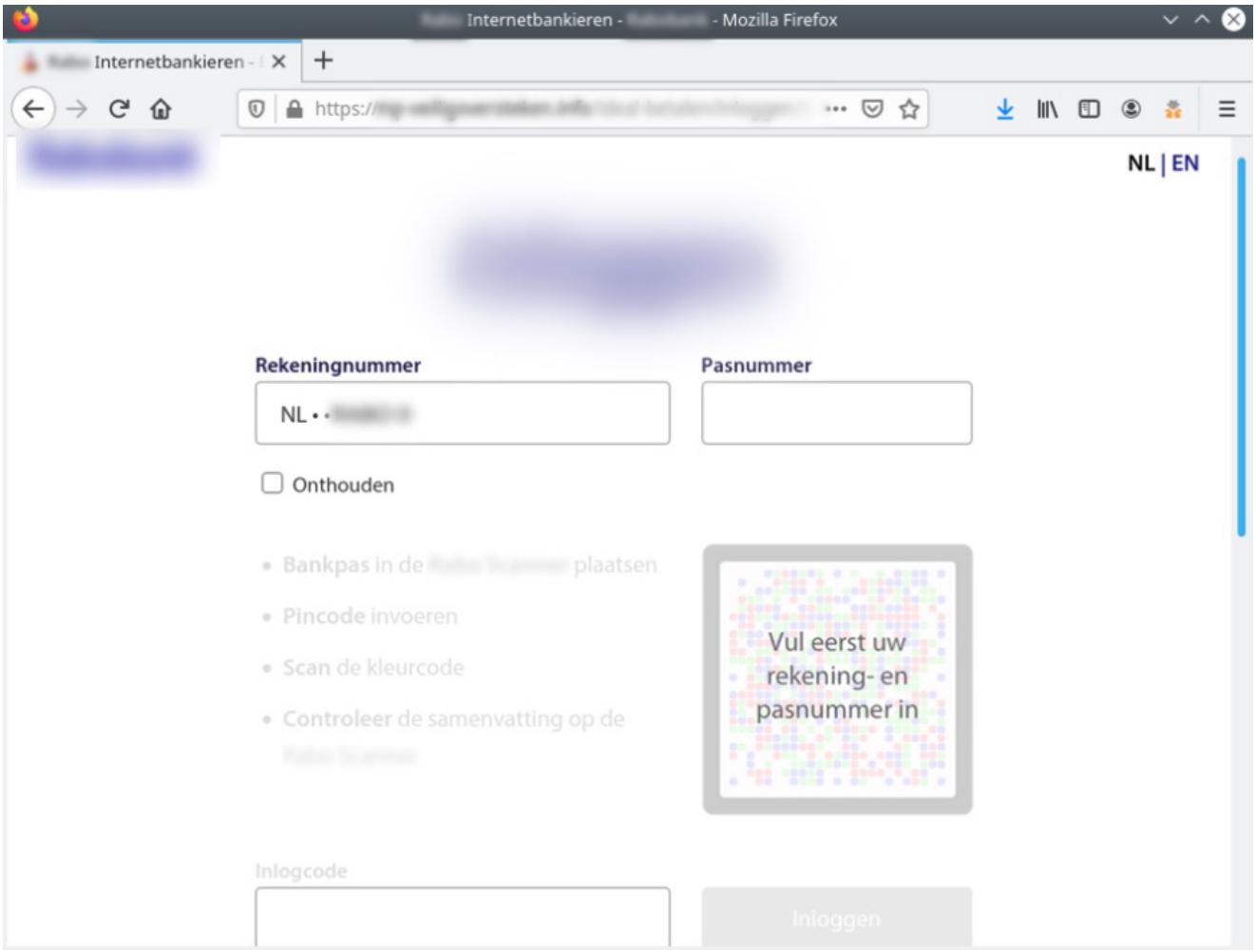


Figure 7 *Phishing website impersonating login interface of a Dutch bank*

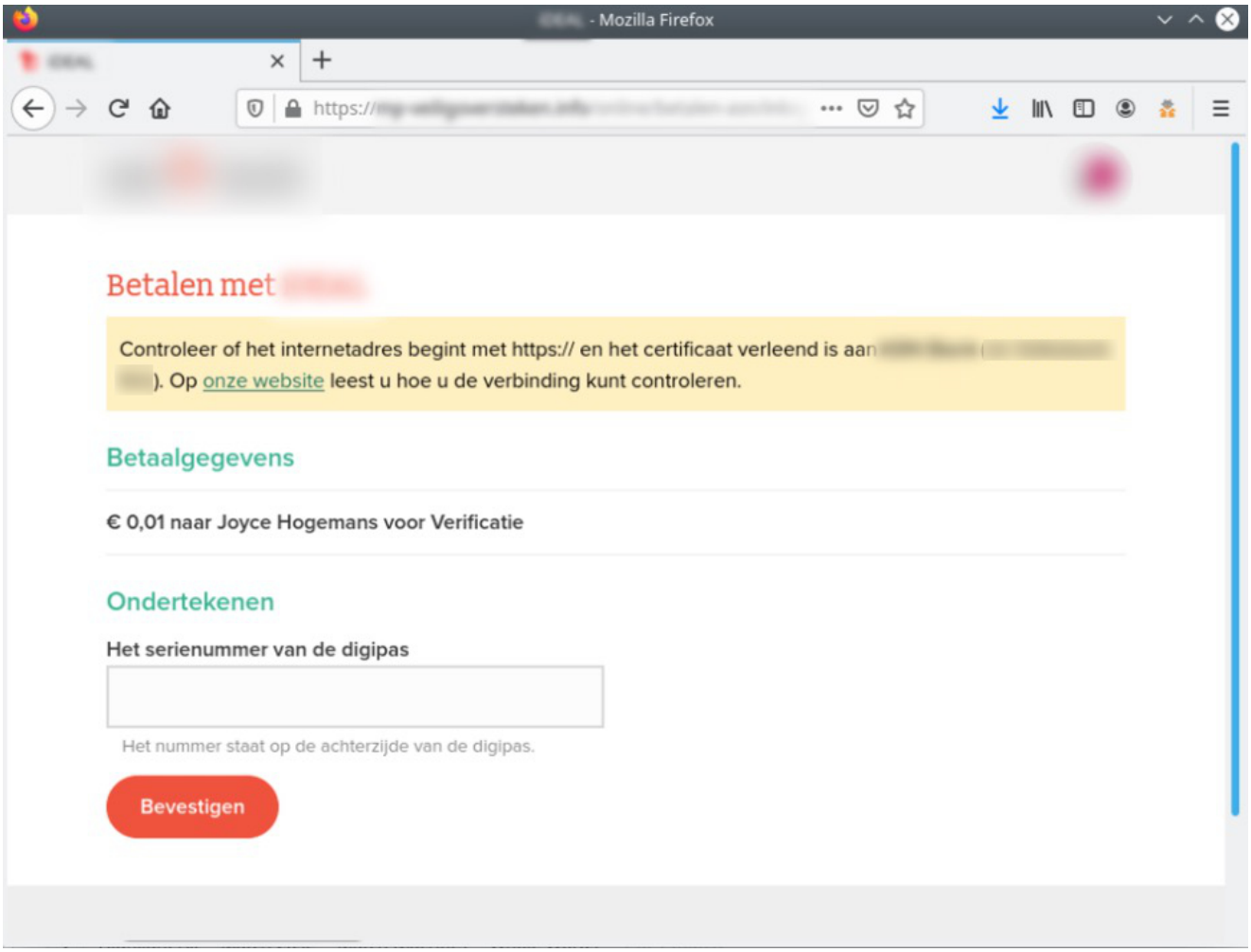


Figure 8 *Phishing website impersonating login interface of a Dutch bank*

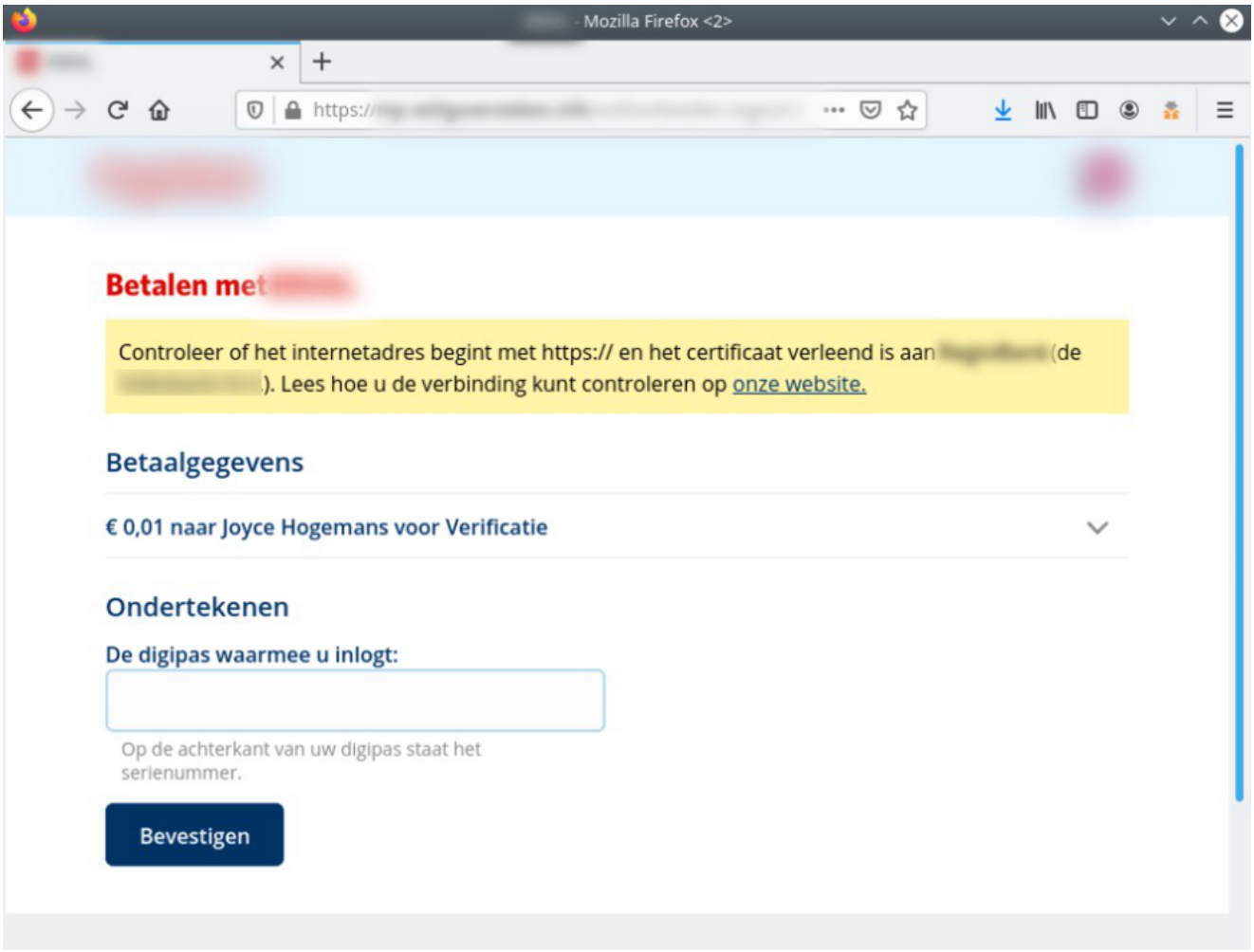


Figure 9 *Phishing website impersonating login interface of a Dutch bank*

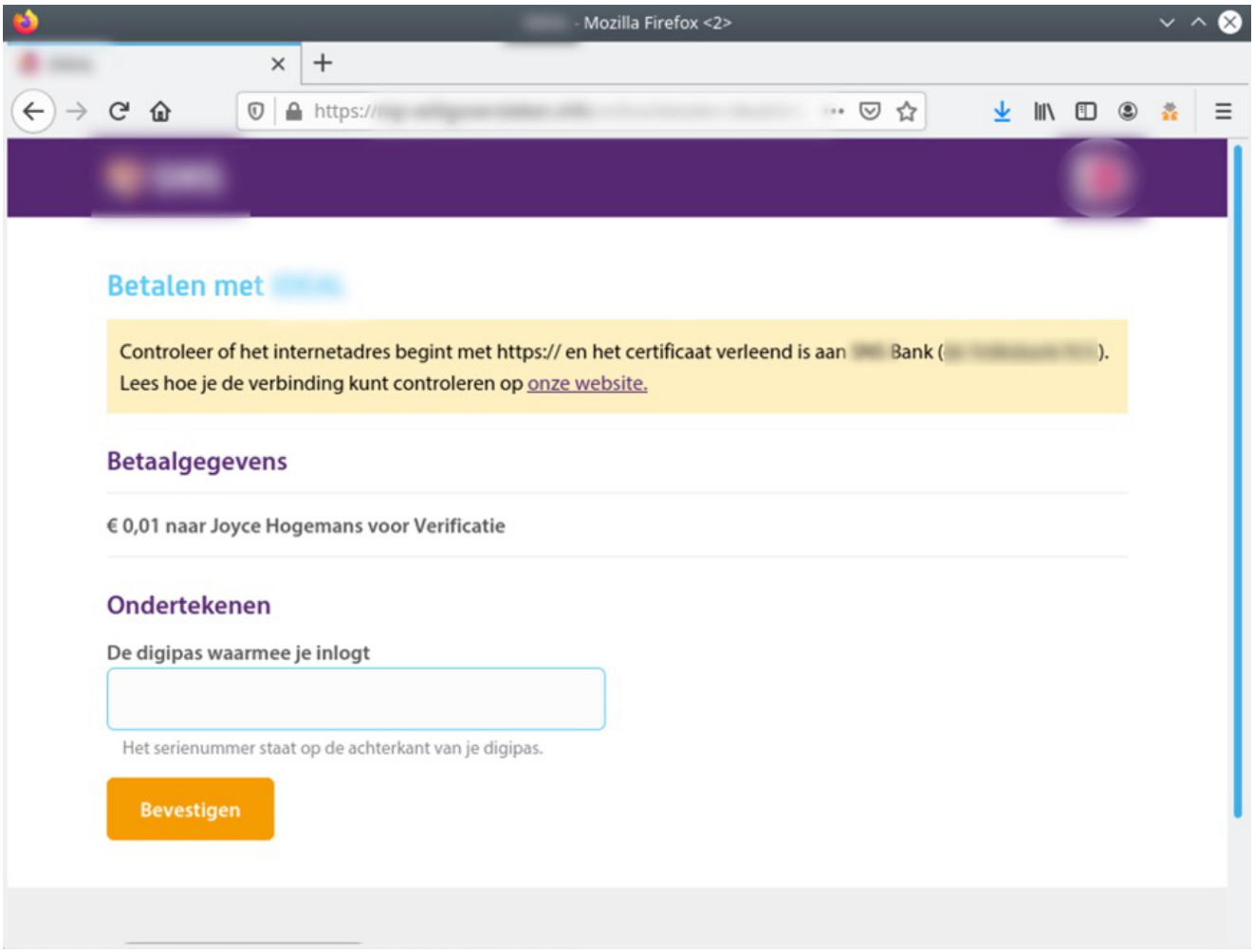


Figure 10 *Phishing website impersonating login interface of a Dutch bank*

The developers of these phishing kits made sure their customers, fellow cybercriminals, could bypass 2FA. The crooks who use this phishing infrastructure get access to a web panel that interacts, in real time, with the phishing site. When victims submit their banking credentials, the phishing site sends them to the fraudster-controlled web panel. This one actually notifies the miscreants that a new victim is online. The scammers can then request additional information that will help them to gain access to the bank accounts, including two factor authentication tokens, and personal identifiable information. While the phishing site is waiting for further instructions from the attackers, the unsuspecting victim is looking at a "Please wait…" screen.

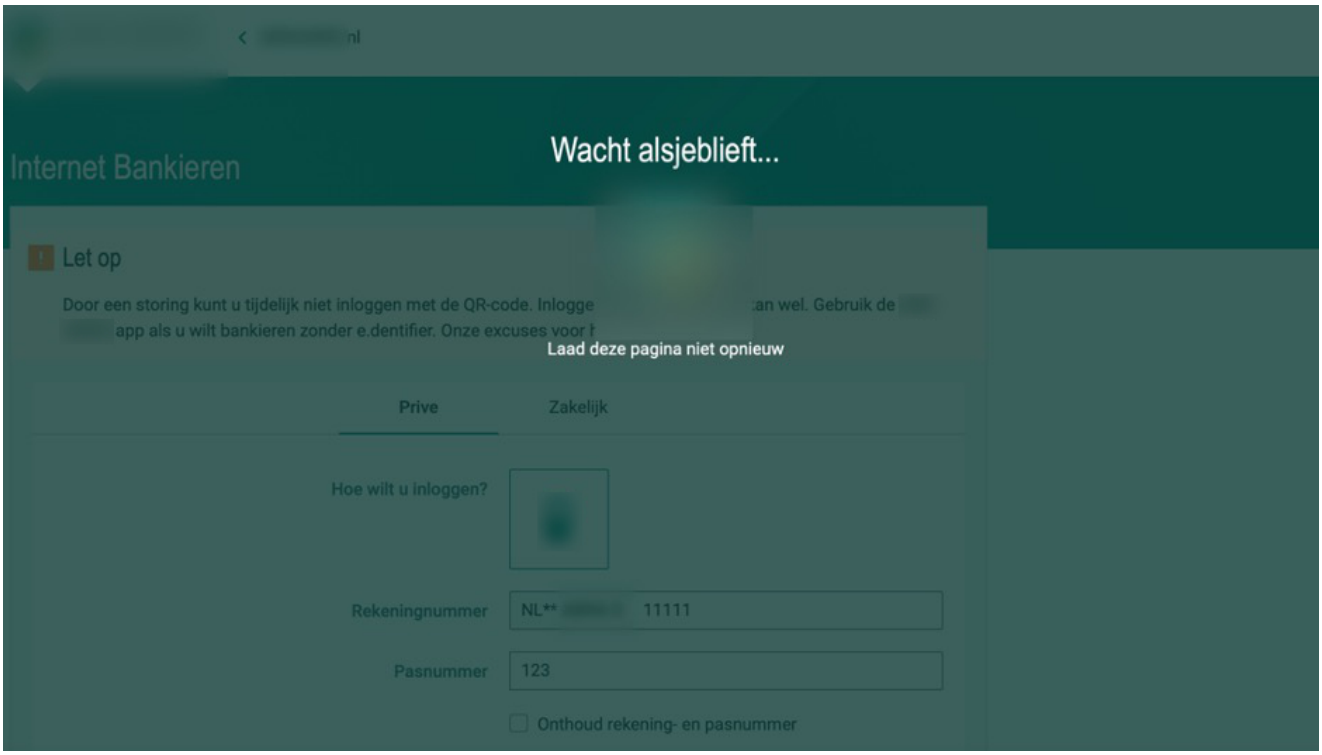


Figure 11 Splash screen showing "Please wait..." message

Group-IB researchers discovered that many of these phishing pages have been developed and supported by a single Dutch-speaking cybercriminal collective, codenamed Fraud Family. In the next section we take a deep dive into Fraud Family's business model, modus operandi and technical analysis of the gang's infrastructure.

Fraud Family's business

Members of the Fraud Family developed a sophisticated fraud-as-a-service infrastructure resilient to conventional takedown efforts. This infrastructure combines ready-to-use phishing frameworks, domains and hosting services that Fraud Family takes care of for less skilled cyber crooks.

The phishing frameworks allow attackers with minimal skills to optimize the creation and design of phishing campaigns to carry out automated fraudulent operations on a mass scale. Phishing frameworks include **phishing kits** — tools and resources used to steal information — and **web panels** that allow cybercriminals to interact with the actual phishing site in real time and are used to collect and manage the stolen user data. The complete "plug and play" phishing service keeps the framework under control and prevents it from leaking to the public.

Members of the Fraud Family actively use **Telegram** as a way to advertise their services to other less skilled fraudsters. These services include the sale of phishing tools, or the rent of "ready to use" infrastructure that comes equipped with the phishing framework and anti-bot

tools to prevent crawlers, automated analysis tools and services like VirusTotal and URLScan, and researchers from accessing the phishing sites. Any fraudster can rent the Express Panel for €200 per month or the Reliable Panel for €250, as seen in Figure 14.

Figure 12 Advertisement promoting the rent of phishing infrastructure

Group-IB cyber investigations team discovered at least **8** Telegram channels operated by the Fraud Family gang. The whole network of channels has close to 2,000 subscribers. Their most popular group has 640 members. According to Group-IB assessment, half of these users could be actual buyers.

Group-IB's research revealed that there are many cybercriminals who are using Telegram to offer phishing frameworks that include fake Dutch and Belgian banks pages and web panels for managing these sites. Many of those plug and play frameworks are being offered with different names and variations.

Deeper analysis showed that the majority of such phishing web panels traded on Telegram are based on U-Admin, which is the panel initially developed by Ukrainian threat actor nicknamed Kaktys.

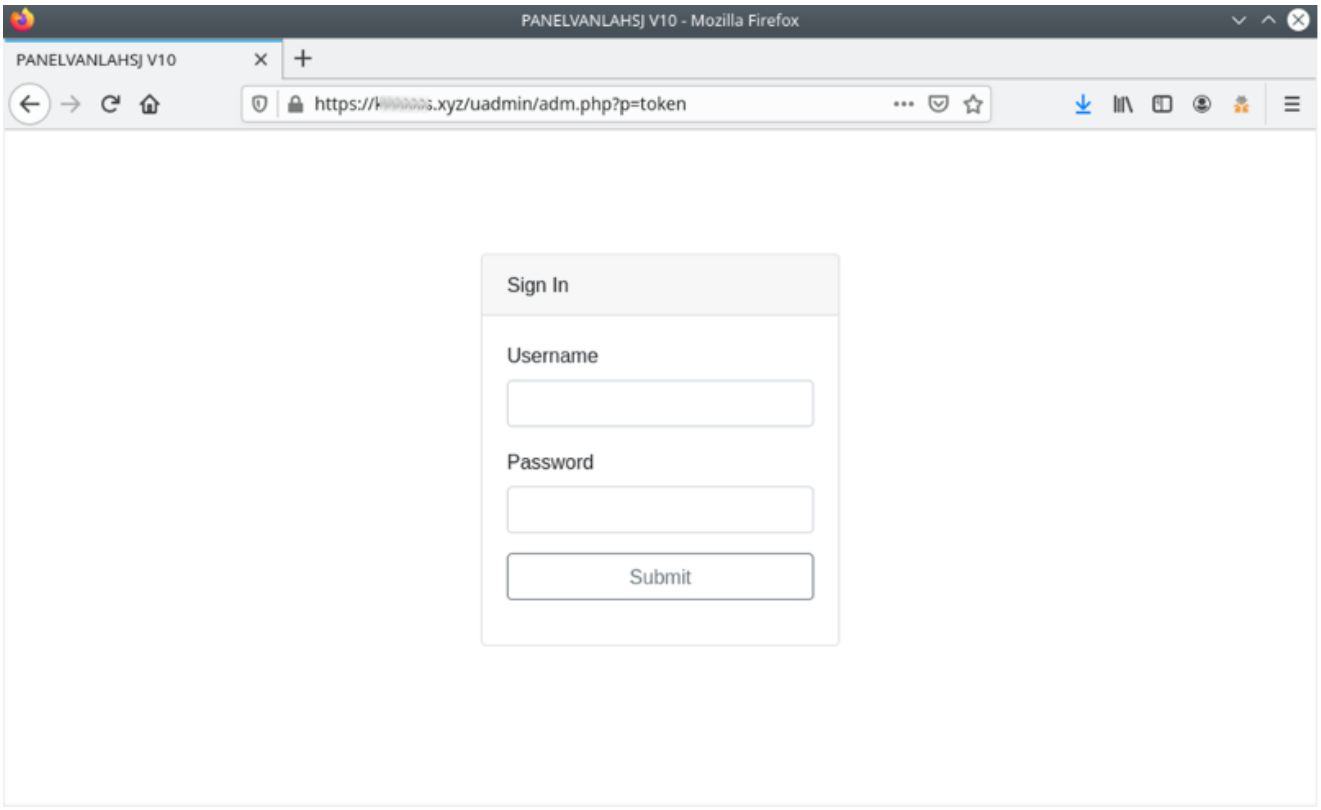


Figure 13 Web panel U-Admin

According to Group-IB's findings, all of the panels designed to target customers of the Dutch and Belgian banks are different versions, or forks, of U-Admin. It turned out that the market of phishing frameworks in the Netherlands and Belgium is being dominated by the Fraud Family. The gang tunes and customizes phishing frameworks like U-Admin and gives them new names.

The most common name given to the panels modified by Fraud Family is NL Multipanel. Two more panels being offered for sale, or rent by Fraud Family are Express Panel and Reliable Panel, developed by the syndicate in 2021.

Group-IB found that the attacks that rely on Fraud Family's infrastructure increased toward the final months of 2020. This trend continues in 2021 with the appearance of Express Panel and Reliable Panel.

The conclusion about the growth of their operations has been drawn from the fact that Group-IB researchers detected more posts and discussion about Fraud Family's business on Telegram.

The detailed analysis of the web panels, modified and customized by the Fraud Family is presented below.

NL Multipanel

NL Multipanel is almost fully based on U-Admin panel, which is offered to a wide range of Exploit.in forum (one of the most popular hacker forums) users. NL Multipanel got its name after being refined and customized by members of Fraud Family to fit the Dutch cybercriminal scene.

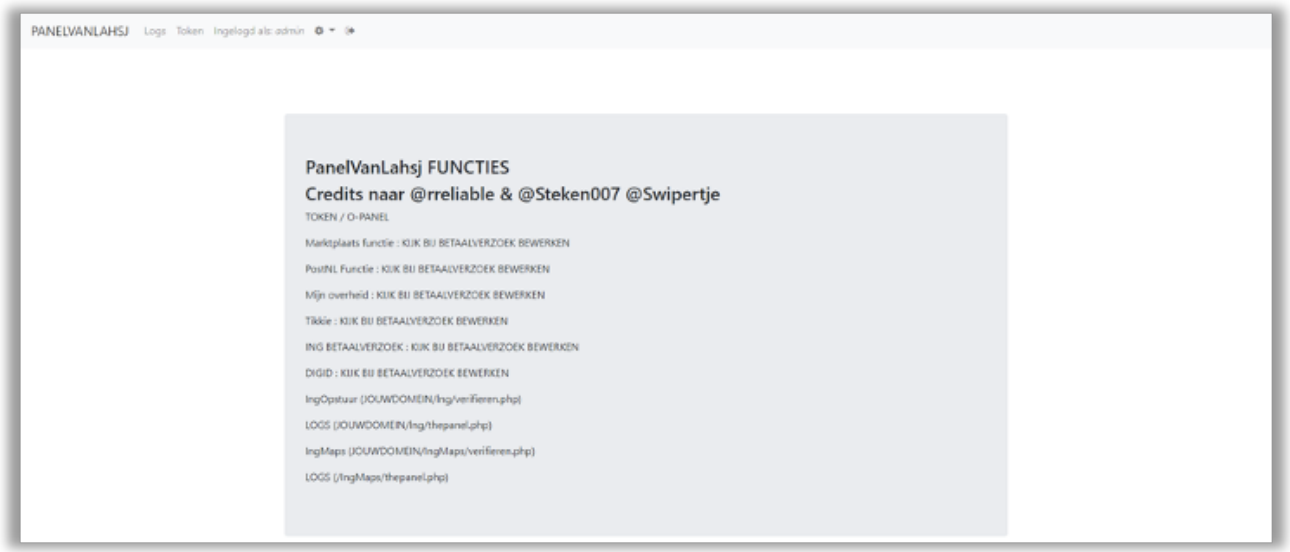


Figure 14 Welcome screen of U-Admin fork "PaneLVanLahsj"

With U-Admin comes a plugin called Token. Because this plugin allows the attackers to interact with their victims in real time, it is the one used to target clients of banks that use any sort of multi-factor authentication.

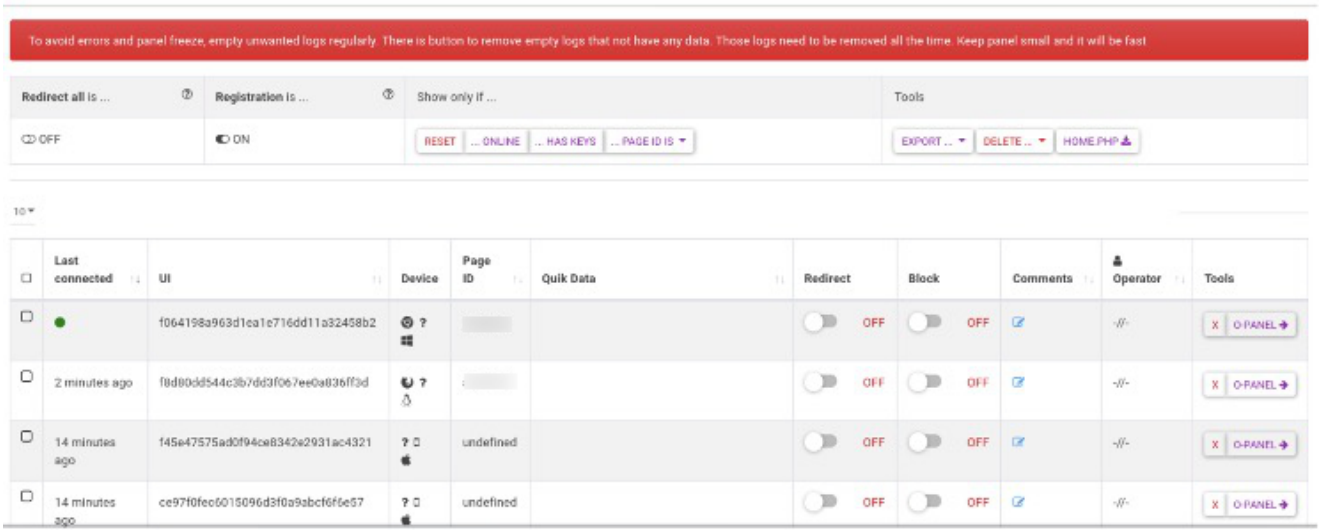


Figure 15 U-Admin Token plugin

When a new victim is online, the attackers use O-Panel to execute a number of operations. This is useful to request any information needed from the victims. While the miscreants use and request new data, victims are waiting for the phishing site to show a new screen asking for this information.

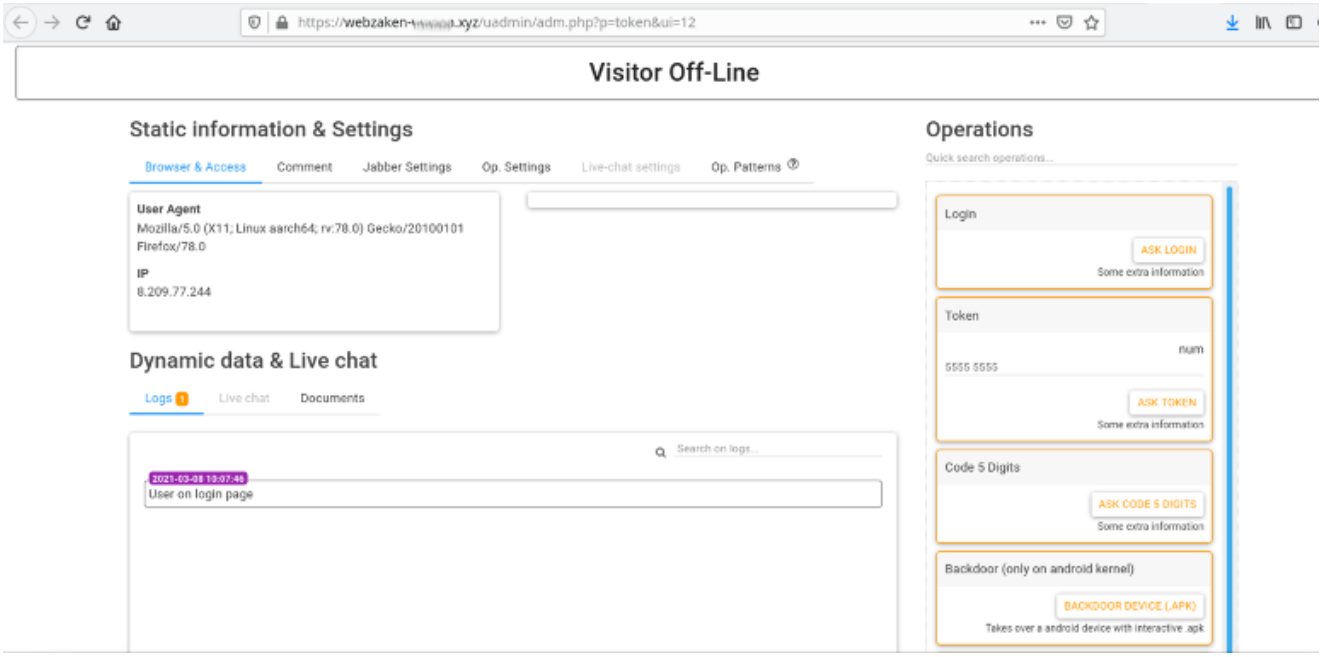


Figure 16 U-Admin O-Panel plugin

O-Panel is very flexible and can be fully customized, by adding new, or modifying existing operations.

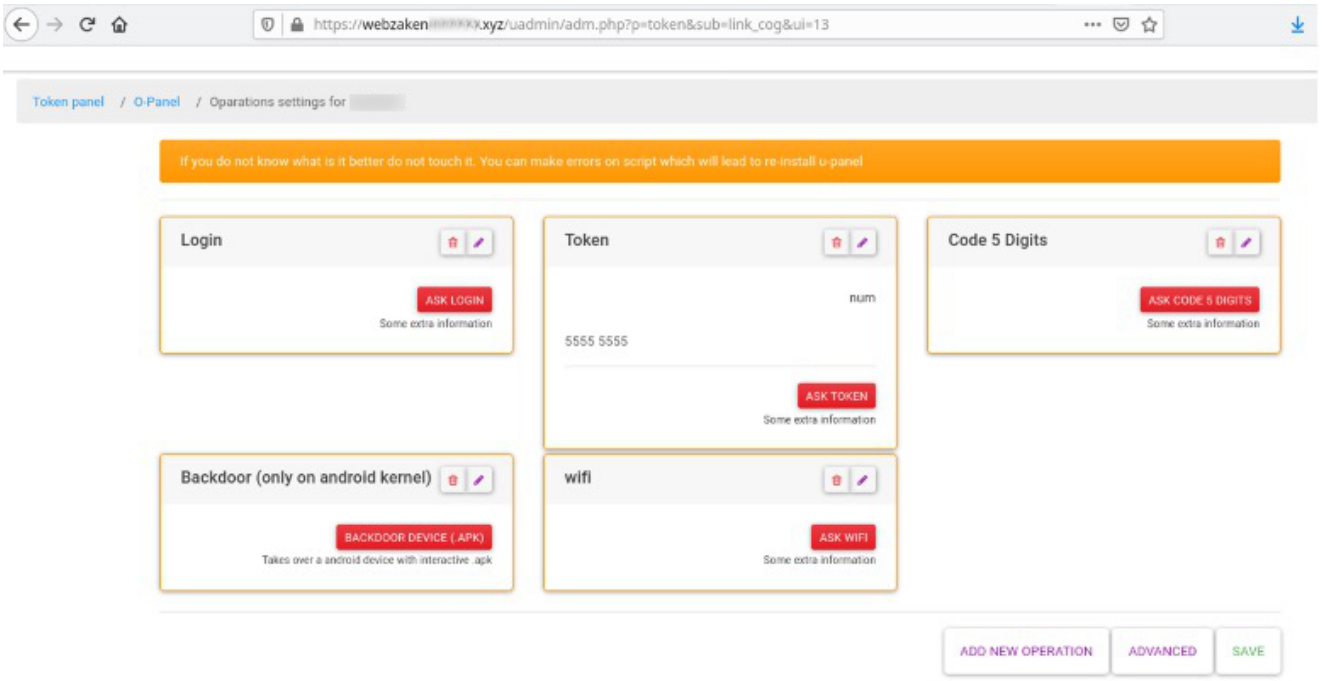


Figure 17 Different operations that can be used with O-Panel

Express Panel

Presumably, this made its public appearance in November 2020. Some of its features include:

- It is not based on U-Admin and sellers make sure to advertise that well

- A very light panel, with a simple user interface
- It is optimized to be used with a mobile phone
- Allows live interaction with victims

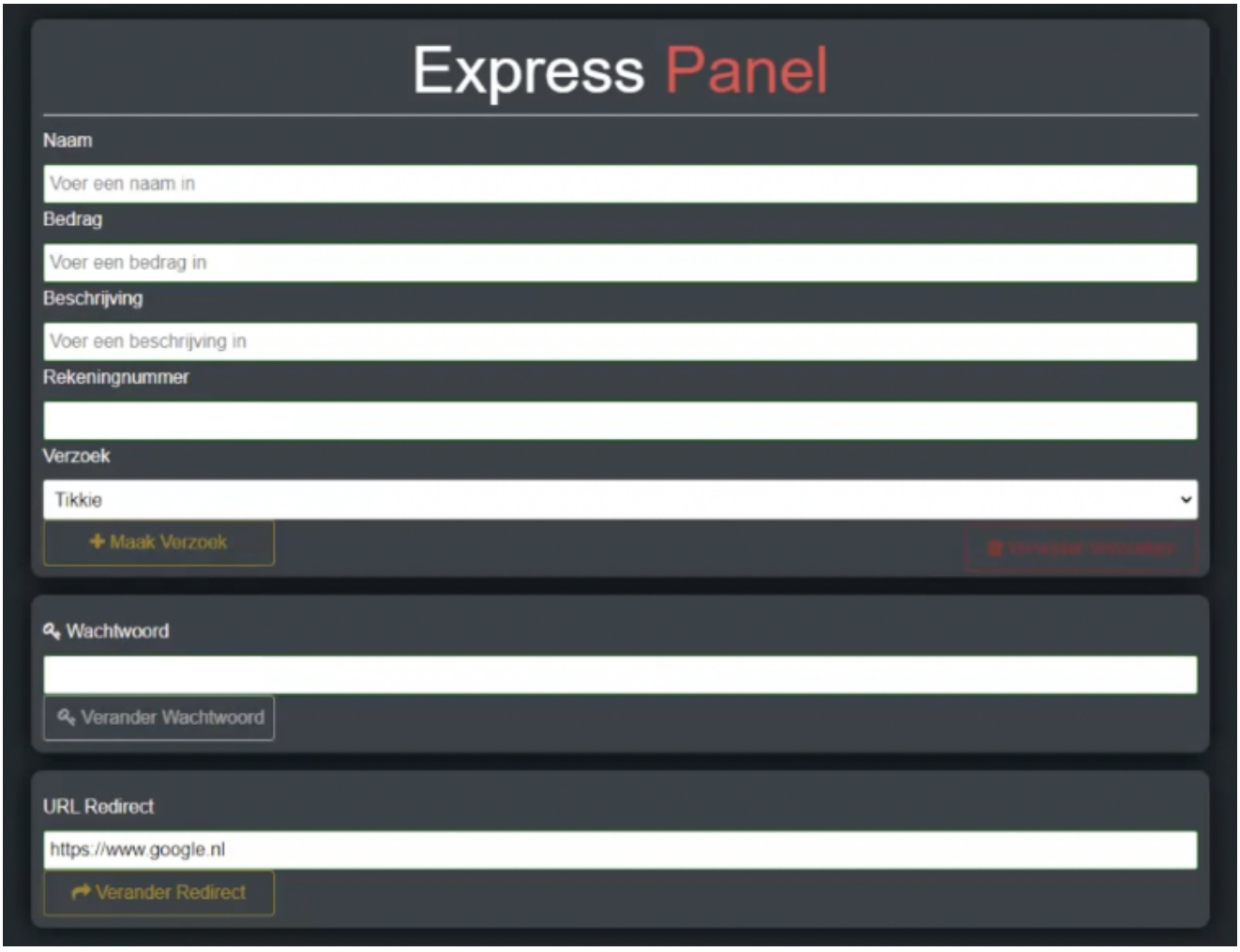


Figure 18 Express Panel as advertised by sellers

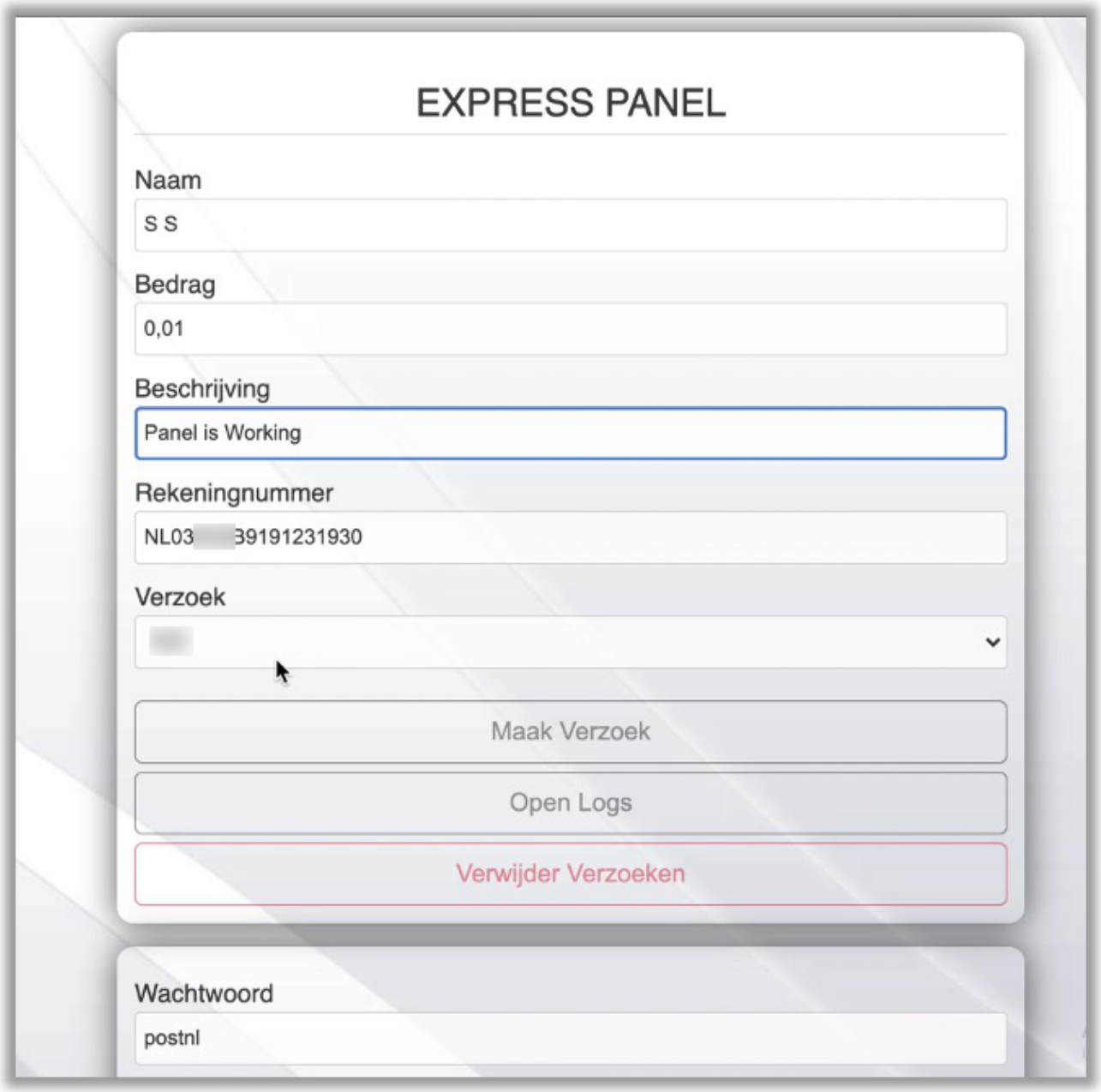


Figure 19 Older version of Express Panel as advertised by sellers

Reliable Panel

It was developed in parallel to the Express Panel by the same developer and also made its public appearance in November 2020.

New features provided by sellers include:

- Developed from scratch and based on Nodejs instead of PHP
- "Lifetime" of about 2 weeks (average time from deployment to take-down)
- Faster that NL Multipanel and its variants
- Fully customizable
- Allows live interaction with victim

Reliable Panel removed many of the weaknesses U-Admin has and is especially crafted for the Dutch and Belgian markets. This phishing framework has the potential to become one of the main tools Dutch cybercriminals can count on.

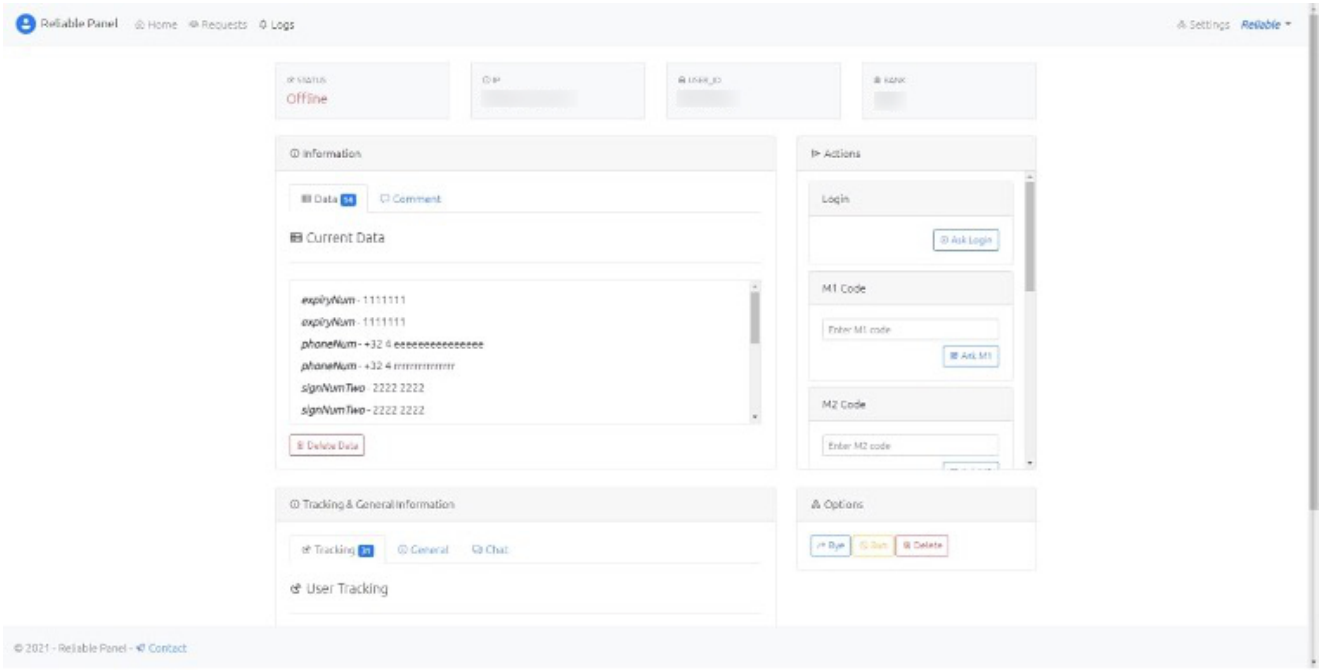


Figure 20 Reliable Panel as advertised by sellers

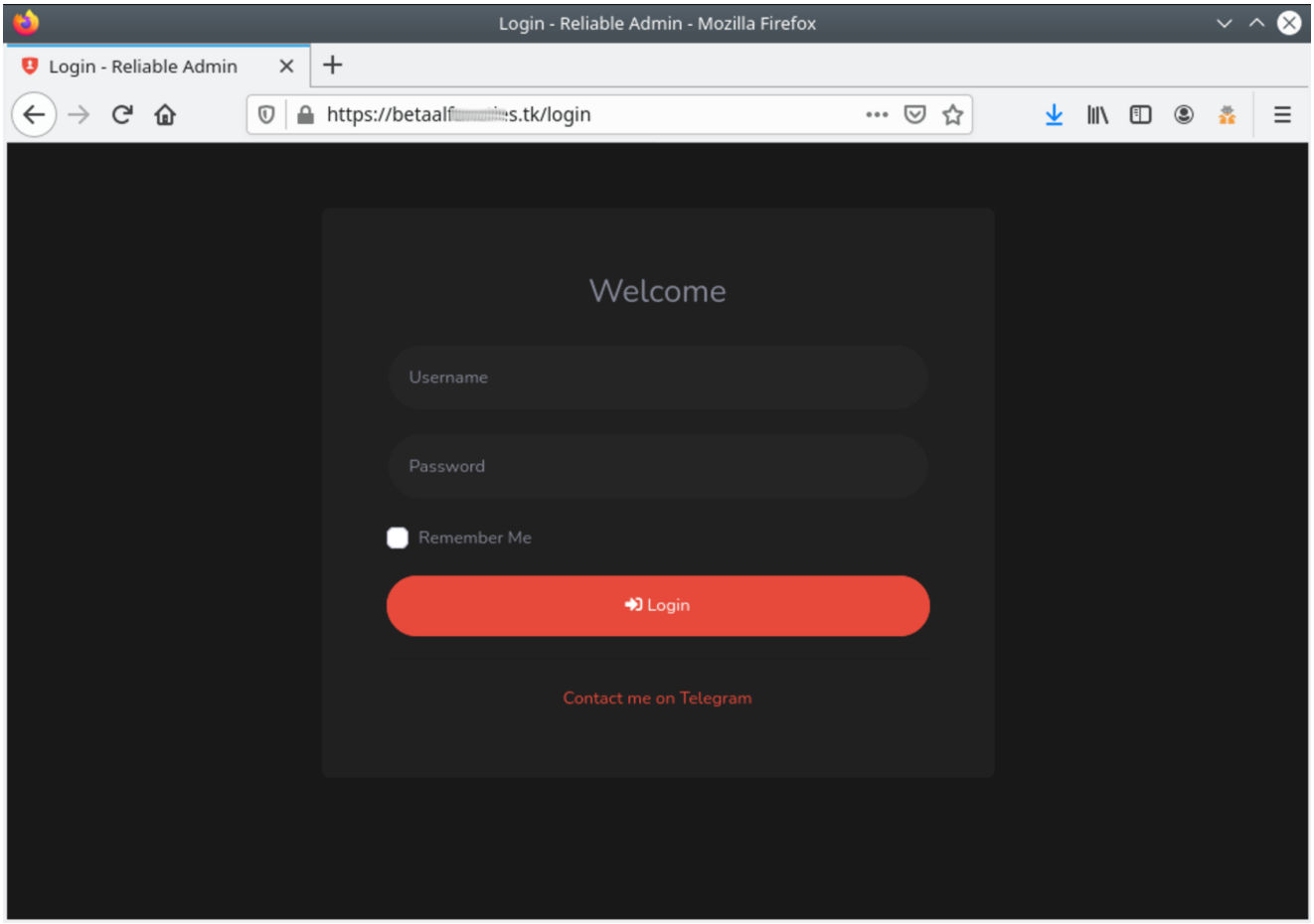


Figure 21 Reliable Admin panel, login interface

It looks like in a more recent version from 2021, the panel was renamed to "Reliable Admin".

Conclusion

Group-IB is actively and closely monitoring the attacks that involve Fraud Family's infrastructure and provides information obtained from them to affected organizations whose brands are being abused by the fraudsters, including leading Dutch financial organizations to help them minimize the amount of fraudulent activity. Group-IB is collaborating with the Dutch Police and also providing information to them on the alleged identities of the Fraud Family members.

In order to help regular users avoid falling prey to Fraud Family's affiliates, Group-IB team prepared a set of simple recommendations:

- Always be cautious and fully aware of anything sent to you, even if you think it may be legitimate.
- Do not click on any links that you are not 100% confident are real
- Double check the address of a website is the official one before you submit any information
- If the link comes from someone you know, confirm with that person using another way of communication
- Contact the organization which sent you a link to confirm they have really sent you that message
- If in doubt, use services like URLScan or VirusTotal to quickly scan the URL you have been sent, and look for red flags
- If you think you may be a victim of a phishing attack, quickly communicate with your bank, the organization being impersonated by the fraudsters and the police. They can issue an alert which may umlimately raise awareness and reduce the victim count
- Keep in mind that usually official organizations do not use URL shorteners, so links leading to bit.ly, s.id, tny.sh and others, are very suspicious and you should double check the final destination
- Report any identified phishing email or SMS to fraudehelpdesk.nl, scamadviser.com. These reports aid cybersecurity professionals to investigate and take action against fraudulent websites, in addition to helping protect other victims.