16.09.2021

RUNLIR - phishing campaign targeting Netherlands

Phishers take an approach to bypass security controls never seen in the country

Reza Rafati
Senior CERT-GIB Analyst, Group-IB Europe

Ivan Lebedev
Head of CERT-GIB Anti-phishing and global cooperation unit, Group-IB

While analyzing a massive phishing campaign aimed at stealing payment data of Dutch residents, the researchers from the Group-IB Computer Emergency Response Team (CERT-GIB) discovered an approach previously unseen in the Netherlands that allows cybercriminals to limit access to phishing websites to only potential victims. By doing this, they ultimately increase the success rate of their fraudulent operations. According to CERT-GIB data, an average phishing page's lifespan is about 24 hours; the phishing pages that used the new approach lived six days on average.

Group-IB analysts identified multiple phishing websites impersonating Dutch financial organizations that are part of a single network of more than **750 connected domains**. The phishing infrastructure was first seen in **March 2021** and remains active until today. The campaign was codenamed **RUNLIR** by Group-IB researchers, as it uses RU, NL and IR in the domain naming pattern. As part of the analysis, Group-IB researchers also observed a very unconventional "Cut the card" phishing scheme that requires fraudsters' efforts both online and offline.

RUNLIR uses the combination unique for the Netherlands that involves the **BlackTDS** anti-bot service, the notorious bulletproof hosting services of **Yalishanda** and different versions of the **uAdmin** phishing kit. This approach ensures that their phishing pages are only shown to victims and not to security professionals.

The cybercriminals use this approach as it allows them to distinguish between unsuspecting victims and security researchers by checking if the page viewer is connecting using a Dutch mobile network to narrow down their reach. Nevertheless, Group-IB researchers quickly established the necessary access conditions and upgraded their Threat Intelligence & Attribution system with a specific proxy server to bypass these restrictions. The approach, discovered by Group-IB CERT analysts, is new and has not been seen in phishing attacks in the Netherlands in the past.

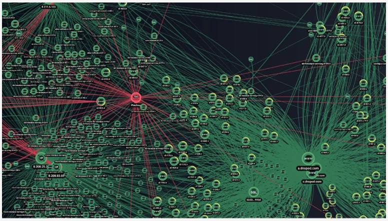
This blog post offers a comprehensive analysis of the unusual phishing campaign in which the unconventional approach was first seen and a detailed description of it.

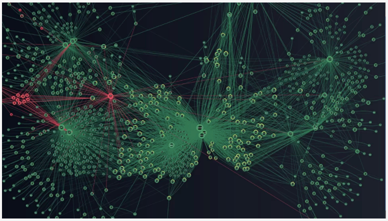
"Cut the card" phishing scheme

Among Group-IB's customers are leading Dutch financial organizations. As part of the regular monitoring and blocking efforts, CERT-GIB analysts discovered a phishing campaign impersonating Dutch financial organizations, including its customers. The campaign, which targeted Dutch residents, began as early as March 2021. CERT-GIB was able to take down those websites related to its customers immediately upon detection.

However, further analysis revealed that these phishing resources were part of a network of more than **750** connected domains used by the criminals to host phishing pages impersonating banks, transportation, logistics, government, telecom, housing, marketplace, and utility companies to target users in the **Netherlands, Germany, Belgium,** and other countries. It must be considered that each of the domains has an average of three subdomains, every one of which is able to host different phishing pages. The campaign was codenamed **RUNLIR** by the Group-IB Threat Intelligence team, due to the phishing domains naming pattern.

The phishing infrastructure shown on the **Group-IB Network Graph** below has been on our radar since March 2021. CERT-GIB eliminated the websites related to its customers and is continuing to monitor the infrastructure as phishing domains tend to reappear after some time.

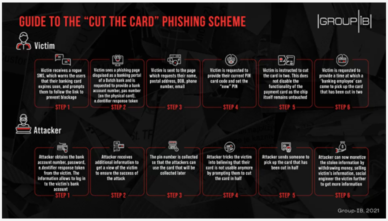




The phishing infrastructure relies on the infamous Yalishanda bulletproof hosting provider and uses the FastFlux technique. This infrastructure is used to make the phishing sites more resilient to take downs by global CERT teams. The sites use the BlackTDS anti-bot service and only accept mobile devices as visitors. The cybercriminals' approach by using the Yalishanda bulletproof hosting in combination with the BlackTDS services allows them to mitigate unwanted eyes on the RUNLIR phishing campaign. BlackTDS is a cybercrime-as-a-service provider that provides the following services: anti-detection, traffic distribution towards exploit kits, availability of domains that can be used for malicious campaigns like phishing. The usage of Yalishanda, BlackTDS and customized forks of uAdmin increases the likelihood of successful campaigns. The detailed analysis of the combination of tools can be found in the next section of the post.

The investigation into the phishing infrastructure itself revealed that various local brands were being impersonated, but there was one specific scheme that caught the attention of our analysts. The unorthodox scheme instructs the victims to cut up their banking cards. It is for that reason that we will take a dive into this phishing attack impersonating one of the Dutch banks.

The specialized 'Cut up your banking card' scheme observed by Group-IB researchers, typically has 5 steps. The victim count is unknown, however, according to Dutch media reports local residents fell prey to a variation of the scheme in June 2021. Below you can find a step-by step guide into the phishing scheme.



GUIDE TO THE “CUT THE CARD” PHISHING SCHEME

Victim

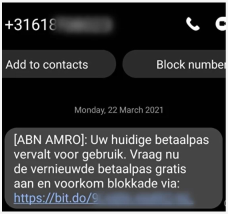
Victim receives a rogue SMS, which warns the users that their banking card expires soon, and prompts them to follow the link to prevent blockage STEP 1
Victim sees a phishing page disguised as a banking portal of a Dutch bank and is requested to provide a bank account number, pas number (on the physical card), e.dentifier response token STEP 2
Victim is sent to the page which requests their name, postal address, DOB, phone number, email STEP 3
Victim is requested to provide their current PIN card code and set the “new” PIN STEP 4
Victim is instructed to cut the card in two. This does not disable the functionality of the payment card as the chip itself remains untouched STEP 5
Victim is requested to provide a time at which a ‘banking employee’ can come to pick up the card that has been cut in two STEP 6

Attacker

Attacker obtains the bank account number, password, e.dentifier response token from the victim. The information allows to log in to the victim’s bank account STEP 1
Attacker receives additional information to get a view of the victim to ensure the success of the attack STEP 2
The pin number is collected so that the attackers can use the card that will be collected later STEP 3
Attacker tricks the victim into believing that their card is not usable anymore by prompting them to cut the card in half STEP 4
Attacker sends someone to pick up the card that has been cut in half STEP 5
Attacker can now monetize the stolen information by withdrawing money, selling victim’s information, social engineer the victim further to get more information STEP 6

Group-IB, 2021

The initial vector, just like with many phishing campaigns, is smishing. The victim receives a rogue SMS impersonating a local organization, which warns the users that their banking card expires soon, and that they need to follow the link in order to prevent blockage. The smishing message also informs the victim that the request to get a new card will be free.



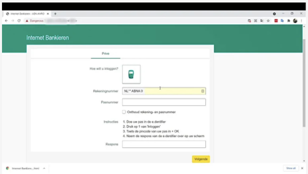
+31618[redacted]

Monday, 22 March 2021

[ABN AMRO]: Uw huidige betaalpas vervalt voor gebruik. Vraag nu de vernieuwde betaalpas gratis aan en voorkom blokkade via: https://bit.do/9[redacted]

Next, after clicking on the link, the unsuspecting victim is requested to provide their banking information, including the e.dentifier response token. The e.dentifier is the physical token tool used by the customers of Dutch banks to generate a secure token, which must be used during the login process. Once the cybercriminals have logged in with the stolen token, they will be in full control of the customer's banking account. In the online banking account, they can see the amount of money the victim has, and they are able to find additional information, such as addresses.

The websites from the screenshots provided below were blocked by the CERT-GIB team immediately upon detection.


Internet Bankieren

Prive

Hoe wilt u inloggen?

Rekeningnummer: NL** ABNA 0

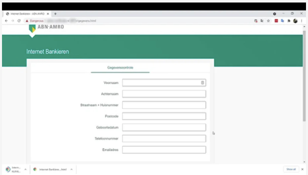
Pasnummer

☐ Onthoud rekening- en pasnummer

Instructies
1. Doe uw pas in de e.dentifier
2. Druk op 1 van 'Inloggen'
3. Toets de pincode van uw pas in + OK
4. Neem de respons van de e.dentifier over op uw scherm

Respons

After the response token is sent to cybercriminals, the phishing website prompts the victim to share all the personal data, including their name, full address, postal code, DOB, phone number, and email address. Phishers often request more information than the minimum that is required. Thus, the crooks have higher chances to capitalize on it by selling the data on the dark web, for example. This information also allows the criminals to perform a quick scan on the web to obtain a photo of their victim, which, if needed, can be used in their attack.


Internet Bankieren

Gegevenscontrole

Voornaam

Achternaam

Straatnaam + Huisnummer

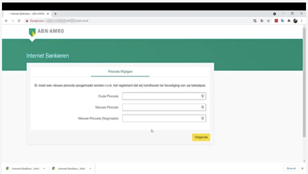
Postcode

Geboortedatum

Telefoonnummer

Emailadres

The criminals then ask the victim to share the PIN number of their existing bank card to use it to steal money later. Additionally, they request that the victim provide a "new PIN code", which leads the victim to believe that they are dealing with the legitimate website of their bank and their existing card is not usable anymore.


Internet Bankieren

Pincode Wijzigen

Er moet een nieuwe pincode aangemaakt worden i.v.m. het reglement dat wij handhaven ter beveiliging van uw betaalpas.

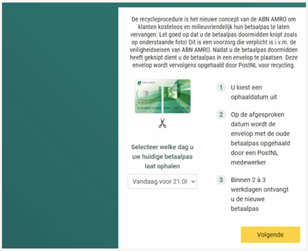
Oude Pincode

Nieuwe Pincode

Nieuwe Pincode (Nogmaals)

Internet Bankieren - ABN AMRO
Dangerous
/pin.html
ABN·AMRO
Volgende
Internet Bankiere....html
Internet Bankiere....html
Show all

In the following step, the victim is instructed to cut the card in two; the cut has to be made through the center of the card. In fact, this step actually does not disable the functionality of the payment card as the chip itself remains untouched. The victim is then requested to provide a 'time' at which a 'banking employee' can come to pick up the card that has been 'cut in two'.


De recycleprocedure is het nieuwe concept van de ABN AMRO om klanten kosteloos en milieuvriendelijk hun betaalpas te laten vervangen. Let goed op dat u de betaalpas doormidden knipt zoals op onderstaande foto! Dit is een voorzorg die verplicht is i.v.m. de veiligheidseisen van ABN AMRO. Nadat u de betaalpas doormidden heeft geknipt dient u de betaalpas in een envelop te plaatsen. Deze envelop wordt vervolgens opgehaald door PostNL voor recycling.

Selecteer welke dag u uw huidige betaalpas laat ophalen

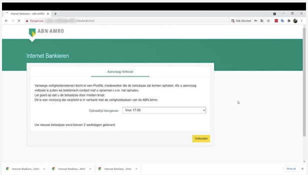
Vandaag voor 21:0(

1 U kiest een ophaaldatum uit

2 Op de afgesproken datum wordt de envelop met de oude betaalpas opgehaald door een PostNL medewerker

3 Binnen 2 à 3 werkdagen ontvangt u de nieuwe betaalpas

In the next step, the victim needs to select a window of time for the appointment with the "bank employee" to take place. This "employee" will come to pick up the card that has been cut in half. This card, of course, remains functional.


Internet Bankieren - ABN AMRO
Dangerous [redacted]/bedankt.html
ABN·AMRO
Internet Bankieren
Aanvraag Voltooid

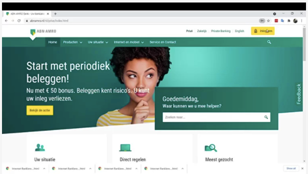
Vanwege veiligheidsredenen komt er een PostNL medewerker die de betaalpas zal komen ophalen. Als u aanvraag voltooid is zullen wij telefonisch contact met u opnemen i.v.m. het ophalen.
Let goed op dat u de betaalpas door midden knipt.
Dit is een voorzorg die verplicht is in verband met de veiligheidseisen van de ABN Amro.

Ophaaltijd Aangeven: Voor 17:00

Uw nieuwe betaalpas word binnen 2 werkdagen geleverd

Voltooien
Internet Bankiere....html
Internet Bankiere....html
Internet Bankiere....html

The last step is the official page and website of the bank that the crooks impersonated. In this stage, the phishers have collected all the information that they need.



Start met periodiek beleggen!

Nu met € 50 bonus. Beleggen kent risico's. U kunt uw inleg verliezen.

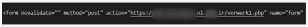
Goedemiddag,
Waar kunnen we u mee helpen?

At the end of this scheme, the cybercriminals have all of the information needed to login and abuse the victim's bank account. The card of the victim can be fixed by simply using some tape, and, as the crooks have access to their bank account, they can come and pick the old card from the victim's physical mailbox.

They are also able to request a new bank card. Just like with a card cut in half, the crooks can get the bank card to the victim's address and pick it up once it has arrived. They will wait for the delivery, and once the card has been delivered, the criminals will force themselves into obtaining the newly sent card.

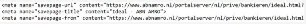
Information theft

When analysing the phishing websites targeted at Dutch residents involved in the RUNLIR campaign, Group-IB researchers discovered that the campaign attempts to steal the user information via ***verwerk1.php***. In this specific PHP file, code is provided that requests the information from the victim via text boxes. Once the values have been provided into the textbox, they will be transferred to the code that is responsible for storing the information.



```
<form novalidate="" method="post" action="https:/[redacted].nl-[redacted].ir/verwerk1.php" name="form"
```

The code itself appears to be a genuine financial environment. It is also worth mentioning that the campaign continues to utilize sources taken from the official target environment. The cybercriminal(s) behind this campaign use this technique as it allows them to quickly set up the phishing resource. Each customization can, of course, be a trigger for the victim to identify that they are dealing with a phishing/malicious site.

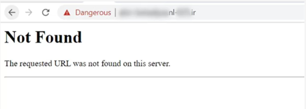


```
<meta name="savepage-url" content="https://www.abnamro.nl/portalserver/nl/prive/bankieren/ideal.html?
<meta name="savepage-title" content="Ideal - ABN AMRO">
<meta name="savepage-from" content="https://www.abnamro.nl/portalserver/nl/prive/bankieren/ideal.html
```

The RUNLIR campaign itself uses a domain generation pattern, which has a preference for utilizing a specific prefix, numeric values, and various top-level domains such as '.IR', and '.RU'.

Cybercrime takes advantage of legitimate security tools

When trying to access resources involved in the RUNLIR campaign from their regular workstation, CERT-GIB analysts would always receive the answer seen below in the image.



Not Found

The requested URL was not found on this server.

Deeper analysis revealed that the phishers were using the BlackTDS GEO tracking service when a visitor tried to access the page.

Cybersecurity professionals use GEO tracking to verify that their users/visitors are from the expected region. For example, a work environment that should only be accessible from the Netherlands does not need to allow connections from Germany. This same concept is now used by BlackTDS to allow cybercriminals to narrow down their reach. There is also a further reason why the criminals might use this technique; it gives them control of the victims they hunt down. We have seen this happen before with Russian malware, which would not run on systems using the Russian language.

Every system with a connection to the web has to make use of an internet routing path, and these internet routing paths are controlled by the Internet Service Provider (ISP). This means that your mobile device will use a different route to a page when compared to a system in the office.

The route can be explained as the system utilizing a different network. Your phone might use the mobile network provided by your mobile internet provider, and your local system might use your home or office network.

The RUNLIR campaign utilizes the following services to block unwanted visitors from their phishing websites and increase the likelihood of successful phishing attempts:

BlackTDS

● They require the browser's user-agent to be a mobile user-agent

● They require the visiting IP address to connect from a mobile network

● They can detect the referrer URL and take action based on that.

● They make use of available domain patterns

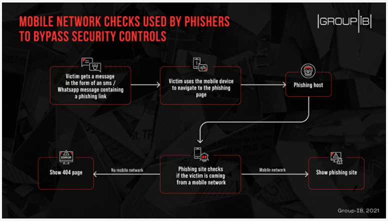
Yalishanda

● Infamous bulletproof hosting service that hinders takedown efforts significantly

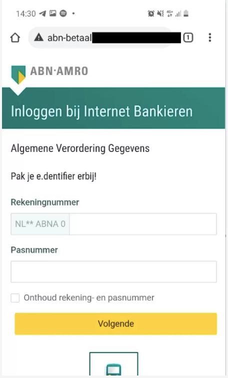
Phishing Kits

● Various versions of the U-Admin phishing panel, 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 phishing campaign uses the combination of the above tools to exclude unwanted visitors, namely cybersecurity researchers and CERT teams, from their websites.


MOBILE NETWORK CHECKS USED BY PHISHERS TO BYPASS SECURITY CONTROLS
GROUP-IB
Victim gets a message in the form of an sms / Whatsapp message containing a phishing link
Victim uses the mobile device to navigate to the phishing page
Phishing host
Phishing site checks if the victim is coming from a mobile network
No mobile network
Show 404 page
Mobile network
Show phishing site
ERROR
Group-IB, 2021

Nevertheless, Group-IB researchers were able to bypass the cybercriminals' detect evasion methods by setting up a proxy that uses mobile networks, and the websites revealed themselves:



Inloggen bij Internet Bankieren

Algemene Verordering Gegevens

Pak je e.dentifier erbij!

Rekeningnummer

NL** ABNA 0

Pasnummer

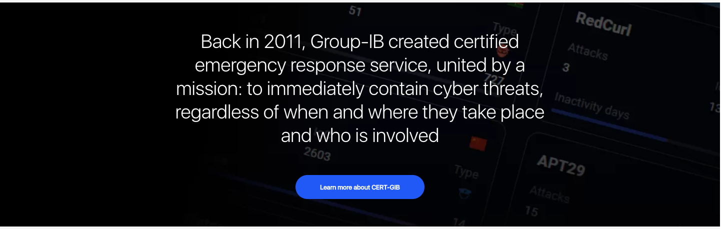
☐ Onthoud rekening- en pasnummer

The fact that cybercriminals have begun adopting this method is a clear indication that the threat actors and their phishing campaigns are continuously evolving. Hence, it's really important to constantly study cybercriminals' TTPs.

Recommendations

Here are some steps that regular users can take to better protect themselves against these types of threats.

1. Do not click on links that you are not 100% confident are real
2. Double check that URL of a website is the official one before you submit any information
3. If you think you may have been a victim of a phishing attack, quickly get in contact with your bank, the organization being impersonated by the fraudsters, and the police. They can issue an alert, which may ultimately raise awareness and reduce the victim count.
4. Keep in mind that usually official organizations do not use common URL shorteners, so links leading to bit.ly, s.id, tny.sh and others, should be treated with suspicion. You should double check the final destination.
5. Always use your official banking application on your mobile device.
6. Report any identified phishing emails or SMS to CERT-GIB, fraudehelpdesk.nl, or scamadviser.com. These reports help cybersecurity professionals to investigate and take action against fraudulent websites, in addition to helping protect other victims.



Back in 2011, Group-IB created certified emergency response service, united by a mission: to immediately contain cyber threats, regardless of when and where they take place and who is involved

Learn more about CERT-GIB

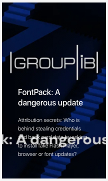
Share

REvil Twins

Deep Dive Into Prolific RaaS Affiliates' TTPs

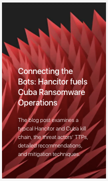
Big airline heist: APT41 likely behind a third-party attack on Air India

Analysis of ColunmTK campaign



FontPack: A dangerous update

Attribution secrets: Who is behind stealing credentials and bank card data by asking to install fake Flash Player, browser or font updates?



Connecting the Bots: Hancitor fuels Cuba Ransomware Operations

The blog post examines a typical Hancitor and Cuba kill chain, the threat actors' TTPs, detailed recommendations, and mitigation techniques.

Company

- About Group-IB
- Media Center
- Leadership
- Contact
- Careers

Products

- Threat Intelligence & Attribution
- Threat Hunting Framework
- Fraud Hunting Platform
- Digital Risk Protection
- Anti-Piracy

Investigation

- Investigations
- Digital Forensics
- eDiscovery

Response

- CERT-GIB
- Incident Response
- Incident Response
- Retainer

Prevention

- Security Assessment
- Red Teaming
- Pre-IR Assessment
- Compromise Assessment
- Cyber Education

Singapore
+65 3159-3798
info@group-ib.ru

Amsterdam
+31 6 225-080-98
info@group-ib.ru