Silent Smishing : The Hidden Abuse of Cellular Router APIs

⋮ 9/30/2025

This article on was originally distributed as a private report to our customers.

Introduction

The monitoring and analysis of vulnerability exploitations are among the primary responsibilities of Sekoia.io's Threat Detection & Research (TDR) team. Using our honeypots, we monitor traffic targeting various edge devices and internet-facing applications.

On 22 July 2025, suspicious network traces were observed via our honeypots. Our analysis revealed that a cellular router's API was exploited to send malicious SMS messages containing phishing URLs — an attack that leverages SMS as a delivery vector for phishing, often categorized under ***smishing*** tactics.

The various messages examined strongly suggest that **Belgium** is being specifically **targeted**, as phishing URLs impersonate legitimate services such as CSAM and Ebox consistently feature the Belgium country code.

Using the Shodan search engine, we identified over 18,000 routers of this type as accessible on the public internet, with at least **572 potentially vulnerable**. Moreover, the API enables retrieval of both incoming and outgoing SMS messages, which indicates that the vulnerability has been actively exploited to disseminate malicious SMS campaigns since at least **February 2022**.

Further examination of the sent messages confirms a deliberate focus on Belgian recipients. However, instances targeting France were also observed. Analyzing the phishing URLs enabled us to identify and track the attacker's infrastructure, which appears to primarily target Belgian users.

This report presents an analysis of the attacker's method to distribute malicious SMS messages. Additionally, it shares insights into the adversary's infrastructure.

Honeypot observation

The attack appears to specifically target **Milesight Industrial Cellular Routers**. Logs collected from internal honeypots indicate the presence of POST requests directed at the /cgi endpoint. The data submitted in these requests is formatted in JSON, with several parameters—particularly those found within the values list—clearly associated with the **sending of SMS messages**.

sekoia | HTTP request request used to send malicious SMS

```
POST /cgi HTTP/1.1
Cookie: loginname=admin; td=[REDACTED]
{"id":1,"execute":1,"core":"yruo_sms","function":"send","values":[{"base":"sms_send","value":
{"destination":"+32[REDACTED]","content":"Er staat een belangrijk bericht in uw eBox hxxps://csam.ebox-
login[.]xyz/?code=[REDACTED] dat uw onmiddellijke aandacht vereist. Twilio","sms_mode":0}}]}
```

A broader review of the honeypot logs revealed multiple occurrences of this pattern. The first traces were observed at the end of June 2025, which corresponds to the deployment date of the Milesight router honeypots. Notably, all the identified requests originated from the IP address212.162.155[.]38, associated with the autonomous system (AS) **Podaon SIA**.

Further analysis of the SMS messages sent via this method reveals:

- A strong focus on Belgian recipients, with message content written in Dutch or French, two of the official languages of Belgium.
- Both phone numbers include the +32 country code, which corresponds to Belgium.
- The phishing URLs typosquat well-known Belgian government platforms, namely CSAM and eBox.

The analysis of all honeypot logs associated with this IP address revealed no additional malicious activity. The attacker appears to focus exclusively on this specific type of equipment, using it solely for the purpose of sending malicious SMS messages.

There is no evidence of any attempt to install backdoors or exploit other vulnerabilities on the device. This suggests a targeted approach, aligned specifically with the attacker's smishing operations.

Vulnerability overview

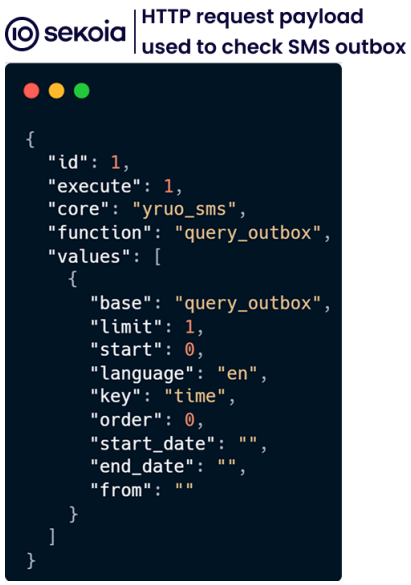
Honeypot logs show that the attacker uses an authentication cookie, suggesting they have valid credentials. A Medium post from October 2023 by a penetration tester, Biptin Jitiya, described a vulnerability –**CVE-2023-43261**– affecting several Milesight industrial cellular routers (UR5X, UR32L, UR32, UR35, and UR41). These devices exposed sensitive log files (*e.g.* system.log, httpd.log) over HTTP without requiring authentication.

The logs contained encrypted administrator credentials, which could be decrypted using **hardcoded AES keys and IVs** found in client-side JavaScript — effectively allowing remote access without authorisation.

API exploitation

The password contained in the authentication cookie observed on our honeypot could not be decrypted using the key and IV described in the article. While this suggests the attacker may have used a different method to obtain valid credentials, the honeypot logs do not show any access to log files. During testing, we found that some routers expose SMS-related features — such as sending messages or viewing SMS history — **without requiring any form of authentication**.

Access to the list of sent SMS messages is performed via a POST request to the /cgi endpoint, using a payload structured as follows:



Retrieving incoming SMS messages works in a similar manner, with the only difference being the substitution of query_outbox with query_inbox in both the function and base parameters.

When unauthenticated access is permitted, the router returns a JSON object containing the timestamp of the SMS transmission, the message content, the recipient's phone number in international format, and a status field (typically *failed* or *success*), which presumably indicates whether the message was successfully sent.

An analysis of the collected data reveals a significant number of SMS messages marked with a *failed* status. Notably, such messages are often repeatedly associated with the same recipient number across different, and sometimes widely spaced, timestamps.

Sekoia.io assesses that the attacker may first attempt to verify whether a given router can send SMS messages by targeting a phone number under their control. This behaviour suggests a validation step, likely aimed at confirming the device's actual ability to deliver messages. In cases where delivery fails, it could be due to various factors, such as SIM card limitations, misconfigured router settings, or insufficient mobile plan allowances.

Even when the router's API is exposed due to misconfiguration, it is possible that SMS functionality may be improperly set up or subject to delivery restrictions. By sending a test message to a controlled number, the attacker ensures that the service is indeed exploitable before initiating broader malicious campaigns.

If this hypothesis proves accurate, it could serve as a valuable indicator for clustering campaigns by attackers.

Vulnerable assets

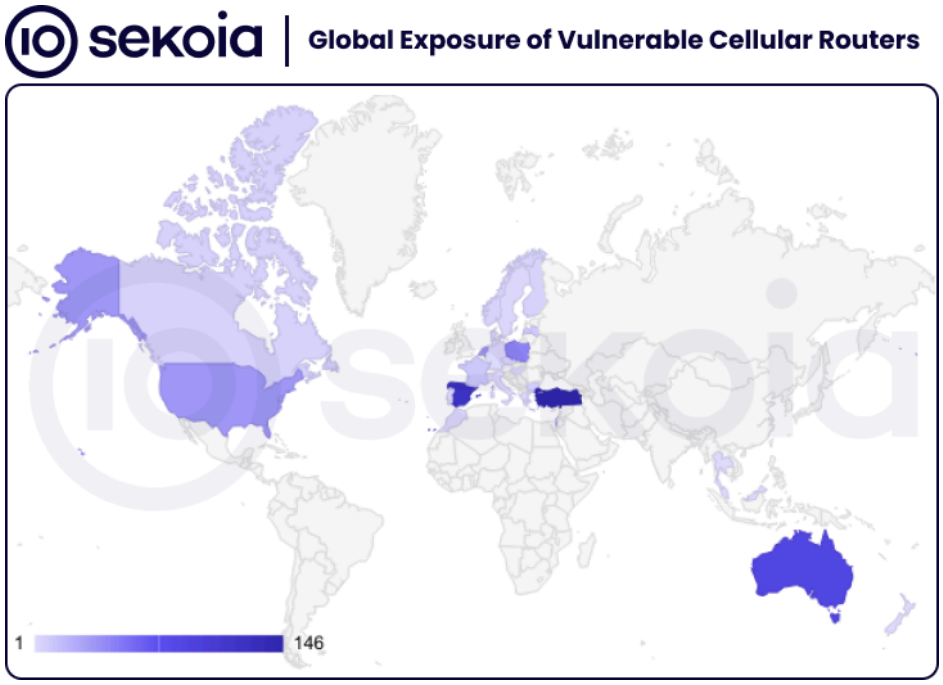
A shodan search revealed the presence of **over 19,000 Milesight Industrial Cellular Routers** devices of this type exposed to the public Internet. Nearly half of these devices are located in Australia. France ranks second, with close to 2,000 assets exposed.

Out of 6,643 assets checked, we identified that **572** of these routers **allow unauthenticated access** to their **inbox/outbox APIs**. These exposed interfaces appear to have been actively exploited to **send malicious SMS messages**, suggesting a widespread abuse of this vulnerability across multiple instances.

The majority of vulnerable routers are be running outdated firmware, with versions 32.2.x.x and 32.3.x.x being the most commonly observed. These versions are known to be affected by multiple vulnerabilities. Interestingly, two devices were also identified as running more recent firmware versions—specifically 41.0.0.2 and 41.0.0.3.

It is worth noting that unauthenticated API access was tested on only a sample of router IP addresses. When combined with other known vulnerabilities—such as those described in the aforementioned Medium article—it is highly likely that credentials could be obtained, potentially allowing for the exploitation of a significantly larger number of devices.

For the routers we were able to identify as accessible, it remains difficult to determine whether access is the result of a specific vulnerability or simply due to misconfiguration—possibly a combination of both.



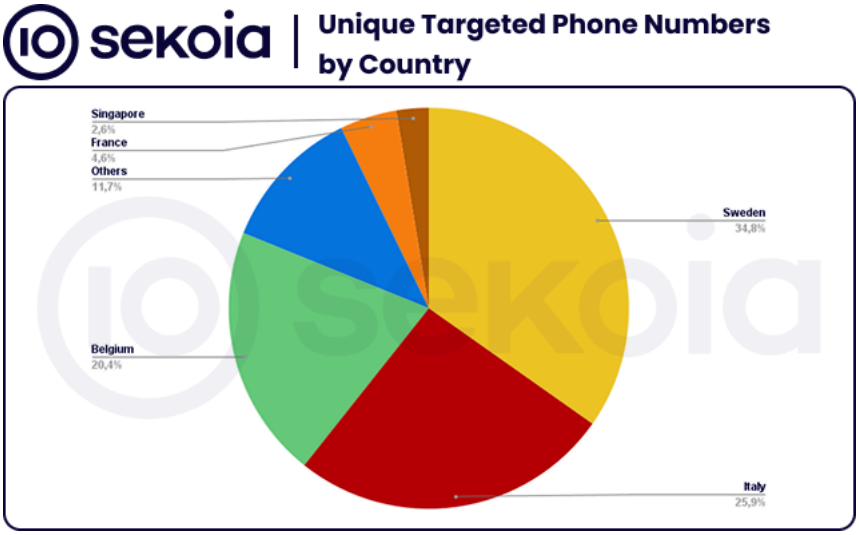
The geographic distribution of vulnerable routers offers noteworthy insights. Turkey, Spain, and Australia are among the countries with the highest concentration of exposed devices. When aggregating the data, nearly **half of** the identified **vulnerable routers** are **located in Europe**.

If the victims' phone numbers are also primarily associated with European countries, this could help explain why European users are being disproportionately targeted. Indeed, the presence of routers physically located in Europe—likely equipped with SIM cards from European mobile operators—would significantly facilitate the delivery of SMS messages to European numbers, both in terms of routing reliability and perceived legitimacy.

Smishing overview

The collected SMS samples include sending dates, with the earliest malicious messages dating back to **February 2022**. This suggests that the vulnerability has been exploited for smishing campaigns since at least that time. The data also indicates that multiple threat actors may be leveraging this flaw.

The analysis of unique targeted phone numbers confirms that Europe is the primary region affected by these malicious SMS campaigns. This likely correlates with the high prevalence of vulnerable equipment located within Europe.



All collected SMS samples are confirmed to be malicious. By extracting the targeted phone numbers, analyzing the sending dates, and comparing the message content, we were able to cluster the messages into distinct smishing campaigns.

As illustrated in the graph above, a large volume of identical SMS messages was sent on the same time interval to 42,044 unique Swedish numbers and 31,353 Italian numbers — indicating mass campaigns launched simultaneously.

In contrast, although fewer Belgian and French numbers were targeted overall, they were affected repeatedly across multiple, distinct campaigns over time. In Belgium, the messages consistently impersonated CSAM and eBox services, whereas the French campaigns used more varied lures and pretexts.

Belgian cases

Based on the collected samples, **Belgium** is very likely the most **frequently targeted** country, with a high number of distinct campaigns observed between November 2022 and July 2025. In most cases, the phishing content impersonates official services such as **CSAM** and **eBox**.

- **CSAM** serves as the official **federal authentication portal** in Belgium, providing secure access to a range of government and administrative services for both citizens and businesses.
- **eBox** is a **centralised digital mailbox** used in Belgium, designed to securely deliver official communications from public authorities to individuals and organisations.

The following table provides representative samples of malicious SMS messages used in the CSAM/Ebox smishing campaigns.

Date	SMS
November 2024	Er is een belangrijk boodschap van CSAM die uw onmiddellijke aandacht vereist t[.]ly/b7alq
April 2025	Er staat een belangrijk bericht in uw eBox hxxps://tinyurl[.]com/3duksme6?code={code} dat uw onmiddellijke aandacht vereist
June 2025	Er staat een belangrijk bericht in uw eBox hxxps://ebox.amltrust[.]cash/?code={code} dat uw onmiddellijke aandacht vereist
June 2025	Vous avez un nouveau document sur votre eBox hxxps://ebox.terugbetaling[.]online/index.html.code={code}
July 2025	Uw jaarlijkse belastingaangifte staat klaar voor verwerking. Zorg ervoor dat u deze voor de deadline indient. hxxps://ebox.csam-trust[.]xyz/?code={code}

NB: hxxps://tinyurl[.]com/3duksme6 *redirect to* hxxps://ebox.dlogin[.]info

Belgium appears to be the only country affected by the most recent campaigns observed in June and July 2025.

French cases

France has also been notably targeted, with several campaigns recorded between October 2022 and March 2025. It is worth highlighting the wide range of impersonated services, spanning postal delivery, social security, and banking payment. Examples of malicious SMS messages are shown in the table below.

Date	SMS
October 2024	AMELI : Votre carte vitale arrive expiration. Effectuez son renouvellement sur le formulaire : hxxps://assurancemaladie-renouvellement[.]info
November 2024	La poste : un problème est survenu lors de la mise en livraison de votre colis, pour plus d'informations rendez-vous sur : logistique-infosms-laposte[.]fr
December 2024	GLS : procédez a la livraison de votre colis sur le lien suivant hxxps://hoo[.]be/lsprmn/1i97xecRxoC
March 2025	CA-Agricole: Activation requise de votre Securipass *Obligatoire Cliquez ici :hxxps://shorturl[.]at/cymM2
March 2025	[Service Opposition]: Vous avez recu (1) nouveau message important, cliquez sur hxxps://urls[.]fr/rUbDjo ou appelez (+33 (0) 03 62 02 11 90)
March 2025	Service Opposition: La transaction de 1490,00 EUR sur le site MARTIGO est en phase de validation. Pour toute question concernant ce paiement, veuillez contacter notre service au 0362021190 ou annuler la transaction sans attendre sur hxxps://service-interbancaire.page[.]dev
April 2025	Votre CB à été bloquée suite a un paiement sur Internet non identifié,ou à un mauvais code secret saisi .contactez +33362021190 (gratuites-24H/24 7j7)

Others

For other countries, the data primarily reveals a single campaign targeting multiple regions simultaneously. Common phishing URLs were observed across these cases, suggesting the same attacker. Examples of malicious SMS messages are shown in the table below.

Date	Country	SMS
May 2025	IT	Non siamo riusciti a elaborare il tuo pagamento. Ti preghiamo di dedicare un momento a controllare i dettagli del pagamento: hxxps://jnsi[.]xyz/IT/#{code}
May 2025	SG	[Grab]: The refund of 88.80 SGD has been processed, please claim your refund before May 20 : hxxps://zpr.]io/kpCrBmPB8wds#{code}
March / April / May 2025	SE	Telia Company: Vi informerar dig skriftligen om att fakturan N-213343 har betalats tva ganger. Du kan begara din aterbetalning harifran: hxxps://estrk.]xyz/SE/#{code}
April 2025	NO	[VippsMobilePay AS]: Vi oppgraderer appen for mer sikkerhet. Bruk lenken: hxxps://is[.]gd/etBhKr#{code}
May 2025	PT	NETFLIX: Nao foi possivel processar o seu pagamento. Reserve un momento para rever os seus dados de pagamento: hxxps://jnsi[.]xyz#{code}
May 2025	HU	Magyar Posta: A linken igazolja kezbesiteset, es azonnal kiszallitjuk hxxps://hotm[.]art/HUDL28128

Phishing infrastructure

CSAM / eBox case

The analysis of of the collected SMS samples led to the following list of phishing domains (excluding shortened URLs) impersonating eBox and CSAM services:

Domain	Registration info	Associated IP(s)	Usage period	Saw in malicious SMS sample
csam.ebox-login[.]xyz	13 Jul 2025 NameSilo	212.162.155[.]45	Active as of 22 Jul 2025	
ebox.plus-billing[.]sbs	27 Jun 2025 NameSilo	212.162.155[.]45	28 Jun – 2 Jul 25	✅
ebox.csam-trust[.]xyz	2 Jul 2025 NameSilo	212.162.155[.]45 212.162.155[.]202	2 Jul – 13 Jul 25	✅
ebox[.]c-sam[.]xyz	23 Jun 2025 NameSilo	185.219.81[.]173 103.246.144[.]60	24 Jun – 22 Jul 25 24 Jul 25	
login.csam-terugbetaling[.]work	18 Apr 2025 NameSilo	185.219.81[.]173	12 Jun – 23 Jul 25	✅
csam.e-box[.]help	Podaon	185.219.81[.]173	18 May – 21 Jul 25	✅
my.ebox[.]help	Podaon	185.219.81[.]173	13 Jun – 23 Jun 25	
ebox.terugbetaling[.]online	3 jun 2025 NameSilo	185.219.81[.]173	3 Jun – 7 Jun 25	✅
ebox.e-login[.]xyz	6 jun 2025 NameSilo	185.219.81[.]173 103.246.144[.]60	6 Jun 25 23–24 Jul 25	

Like the IP address observed in the honeypot logs—used to exploit the router API for sending phishing SMS messages—these domains are associated with IP addresses belonging to **PODAON-PL-1** (AS210895). This suggests that the attacker consistently relies on NameSilo for domain registration and hosts their infrastructure with Podaon, SIA.

Podaon is a Lithuanian company that provides VPS (Virtual Private Server) services, which are leveraged as part of the attacker's operational setup.

Phishing analysis

As of 23 July 2025, the page csam.ebox-login[.]xyz is still active and was subjected to further analysis. Upon accessing the page, a JavaScript file located at /static/detect_device.js is retrieved. In addition to generating a session cookie, the script primarily checks whether the page is being accessed from a mobile device using the condition 'ontouchstart' in document.documentElement.

The resulting boolean value is sent to the server via a POST request to the /detect endpoint, under the key is_mobile. The page is then refreshed. If is_mobile is true, the phishing page is displayed; otherwise, the server responds with an HTTP 500 error.

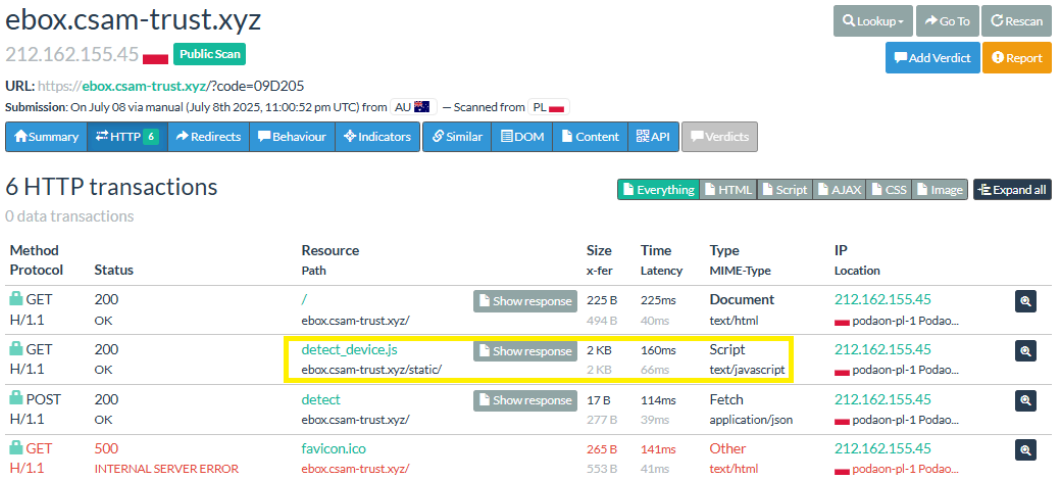
Since the URLs are distributed via SMS, it is clear that the attacker is targeting mobile devices. This mechanism is likely designed to prevent access from non-mobile environments—potentially to evade detection in sandboxes or automated analysis tools.

CSAM Phishing page

The displayed page impersonates the Belgian CSAM service. It states "Update your information for the reimbursement of public services". **Its aim is to steal the target's banking information**.

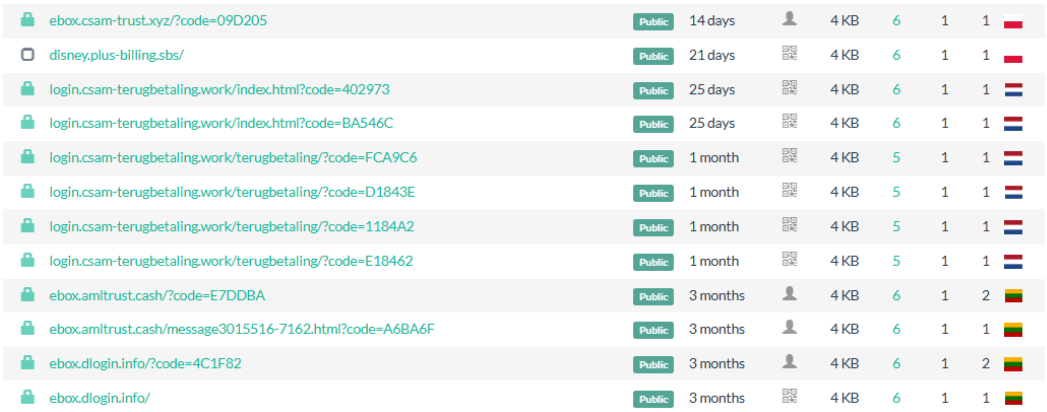
Heuristic tracking

Older domains were also queried via the urlscan.io service. The domain ebox.csam-trust[.]xyz was submitted, and its behaviour mirrors that of csam.ebox-login[.]xyz



ebox.csam-trust[.]xyz url scan analysis

URLScan receives an HTTP 500 response, most likely because the is_mobile value returned is set to false. This behaviour could potentially serve as a tracking mechanism. The heuristic filename:"detect_device.js" AND page.status:500 proves effective in identifying multiple phishing pages exhibiting similar behaviour. Notably, several of these pages also appear in the collected malicious SMS samples.



urlscan.io results from heuristic

All of these domains are represented in the collected SMS samples. While disney.plus-billings[.]sbs does not appear to impersonate CSAM or eBox services, it is still linked to the same attacker and hosted on the same infrastructure. The smishing lure used in this case references a payment issue that requires the victim to click on a provided URL to resolve it. These messages were sent to U.S. phone numbers, suggesting that the attacker is not exclusively targeting Belgian users and may be operating multiple phishing kits tailored to different themes and regions.

Refund / Payment process case

In the campaigns that targeted multiple countries between January and April 2025, the general theme of the SMS messages remained consistent, typically relating to payment issues. It was also observed that a particular domain — jnsi[.]xyz — was used across several of these campaigns. This domain was registered on 8 April 2025 and is associated with the IP address 82.147.84[.]79, which belongs to **AS211860**, a relatively new Russian autonomous system.

This IP address also resolved to the domain estrk[.]xyz, which was observed in smishing samples targeting Sweden. In these SMS messages, the sender was spoofed to appear as the Swedish telecom operator **Telia**.

It is also worth noting that, during the same period, this IP address was associated with several other highly suspicious domains — some of which also impersonated **Telia**, further supporting the link between the infrastructure and ongoing smishing activity.

- `telia-online-service-n382322323[.]ydns[.]eu`
- `telianorge[.]duckdns[.]org`
- `telianorge[.]onthewifi[.]com`
- `qynyuonline-telias-n2689829292[.]jnsi[.]xyz`
- `booking-confimraition-28732893[.]duckdns[.]org`

- www[.]netflix-online-service-n26382932[.]duckdns[.]org
- postcanada[.]booking-review-n32789283[.]duckdns[.]org
- spotify-online-s[.]ydns[.]eu
- kundlingpostbe[.]bounceme[.]net
- www[.]mail[.]klentbeposting[.]duckdns[.]org
- online-mobilepey-n2637832h23[.]beju[.]info
- www[.]post-israel-online-service-8327328982392[.]opensuc[.]com

Grooza cluster

A search on urlscan.io for jnsi[.]xyz domain reveals the FQDN online-telias-n2689829292[.]jnsi[.]xyz, which was scanned in May 2025 — aligning with the period of smishing activity. Urlscan.io classifies the site as malicious, and the screenshot confirms that it impersonates **Telia**. The urlscan.io analysis also shows that the page loads a JavaScript file named maghat_lebssouch.js, which may serve as a valuable pivot point for further investigation.

```
filename:"maghat_lebssouch.js"
```

This obfuscated script is designed to hinder analysis of the phishing page — its primary function is to disable right-click actions and browser debugging tools, thus impeding efforts by analysts or automated scanners to inspect the HTML, DOM, or network behaviour of the page.

Analysis of this JavaScript script reveals additional indicators or patterns, including *GroozaV2* and a reference to the file:
hxxps://gist.githubusercontent[.]com/GroozaV2/ad6936ea84c50c368d4e0454247c5cba/raw/621e078ec9966ea40adffceaf0d1e23f8ad73183/by

At the time of writing the resource is down and the more recent one used https://cdn.jsdelivr[.]net/gh/GroozaV2/my-styles/audiio.js is also down.

```
filename:"filename:"gist.githubusercontent.com/GroozaV2/" OR
hash:62e9e09879ad08e04c4809475407f30d3ba22da53231f11aa1673c99c1225e94 OR
filename:"cdn.jsdelivr.net/gh/GroozaV2" OR
hash:63dad92479c34dde8849303d879ede3b6dc9cd87d07916c1a4f188eaea92d72b"
```

These two ressourcers also serve as useful pivots, enabling the identification of numerous phishing pages. Pivots on this infrastructure highlight some domains that appear to be compromised rather than registered by the intrusion-set. Indicators of compromise (IOCs) related to this threat are provided as full URLs to reduce the risk of false positives when used in detection systems or blocklists.

Throughout the observed campaigns, the threat actor impersonated a range of legitimate organisations to increase the credibility of their smishing and phishing lures. The following legitimate services were mimicked:

- Telia – Swedish telecom provider
- TV2 Denmark – Danish public television broadcaster
- SWICA – Swiss health insurance provider
- SwissPass – Swiss national transport subscription system
- ICS (International Card Services) – Dutch credit card issuer
- MitID – Denmark's national digital identity solution

Some phishing pages linked to this cluster have been observed integrating Telegram as a channel to log visitor connections. These pages utilise a Telegram bot named "GroozaBot", which is operated by a user with the handle "Gro_oza". This account name aligns with the "Grooza" references embedded within the earlier JavaScript artefacts, suggesting continuity between infrastructure, tooling, and operator identity.

Insights from limited Telegram conversations involving this user — along with linguistic artefacts found in the JavaScript logging text — indicate that the operator appears to speak at least Arabic and French. Additionally, the user's Telegram profile picture was taken in Thailand, indicating the presence of the actor at some point in time.

Conclusion

Smishing continues to represent a significant and evolving threat in the landscape of digital fraud. This form of attack leverages text messaging to deceive individuals into divulging sensitive information, such as banking credentials, often by impersonating trusted institutions. Targeting individuals for financial fraud through phishing remains a classic and highly effective technique — one that is easily accessible to low-skilled threat actors thanks to the widespread availability of phishing kits, delivery services, and underground marketplaces. Despite its simplicity, this method can be highly profitable, making it a persistent vector in cybercriminal operations.

In the case under analysis, the smishing campaigns appear to have been conducted through the exploitation of vulnerable cellular routers — a relatively unsophisticated, yet effective, delivery vector. These devices are particularly appealing to threat actors as they enable decentralised SMS distribution across multiple countries, complicating both detection and takedown efforts. The ability to send messages at scale without being flagged as malicious is one of the core operational challenges in smishing. Automating this process, maintaining high throughput, and evading filtering systems are key constraints that attackers must overcome. This campaign is notable in that it demonstrates how impactful smishing operations can be executed using simple, accessible infrastructure. Given the strategic utility of such equipment, it is highly likely that similar devices are already being exploited in ongoing or future smishing campaigns.

In light of this, heightened vigilance remains essential. Users should be cautious of unsolicited messages — especially those containing shortened or suspicious URLs, spelling or grammatical errors, or urgent calls to action. Awareness and scepticism are among the most effective defences against smishing attempts, which increasingly target both individuals and organisations on a global scale.

IoCs

CSAM/Ebox – Domains

```
csam.ebox-login[.]xyz
ebox.e-login[.]xyz
ebox.plus-billing[.]sbs
ebox.csam-trust[.]xyz
ebox[.]c-sam[.]xyz
login.csam-terugbetaling[.]work
ebox.c-sam[.]xyz
csam.e-box[.]help
my.ebox[.]help
ebox.terugbetaling[.]online
ebox[.]amltrust[.]cash
my[.]ebox[.]help
csam[.]pages[.]dev
ebox-vipps[.]pages[.]dev
ebox[.]pages[.]dev
ebox[.]dlogin[.]info
```

Others – Domains

```
disney[.]plus-billing[.]sbs
service-interbancaire[.]pages[.]dev
opposition[.]online
assurancemaladie-renouvellement[.]info
logistique-infosms-laposte[.]fr
```

GroozaV2 – URLs

```
vhxxps://alpyateknoloji[.]com/wp-backup/
hxxps://shaliyah[.]co[.]za/backup/
hxxps://sv-management[.]olekgs[.]nl/en/home/verification[.]php
hxxps://awladlktoccyat[.]ortomanalessia[.]com/ppl-it/mark[.]php
hxxps://lb-prm[.]blogspot[.]com/
hxxps://auth-simply[.]grupositel[.]com/simply/mark[.]php
hxxps://auth-billing-smp[.]grupositel[.]com/simply/mark[.]php
hxxps://urlocalartist[.]pt/mit/
hxxps://superluckbet[.]com/bonus/
hxxps://avrasyaproje[.]com[.]tr/backup/
hxxps://mcaluminios[.]pt/refresh/
hxxps://sv-management[.]ogveranda[.]com/wix/verification[.]php
hxxps://acountinteruption[.]diprimiocostruzioni[.]it/ppl-it/mark[.]php
hxxps://luis[.]com[.]ve/mail/
hxxps://metodorsame[.]sinistraperisraele[.]com/ppl-it/mark[.]php
hxxps://edizhoca[.]com/wp-backup/
hxxps://sv-management[.]aaltink[.]com/wix/verification[.]php
hxxps://afpsat[.]pt/cbb/
hxxps://sv-management[.]eco-fin-service[.]it/wix/verification[.]php
```

hxxps://ilkeevingencel[.]com/app/
hxxps://airprint[.]gr/kund/
hxxps://sercicio[.]paypl[.]studiolegaleflm[.]it/ppl-it/mark[.]php
hxxps://alkodi[.]gr/backup/
hxxps://alkodieshop[.]gr/up//
hxxps://alkodieshop[.]gr/up/
hxxps://alkodi[.]gr/kund/
hxxps://valeriatari[.]com/mytv/
hxxps://wheelmedia[.]hu/wheelmediahu/
hxxps://alexismaidana[.]com[.]ar/padron/
hxxps://dewa-ae[.]mandegroupeinternational[.]org/gov/verification[.]php
hxxps://sanremomotors[.]co[.]za/wp-mail/
hxxps://outprint[.]pt/dk/
hxxps://nwminingindaba[.]co[.]za/Kunden/
hxxps://www[.]afpsat[.]pt/cbb/
hxxps://chissema[.]com/backup/
hxxps://naprakeszingatlan[.]hu/wp-mail/
hxxps://vmaxmagazin[.]hu/wp-mail/
hxxps://www[.]afpsat[.]pt/cbb/index[.]php
hxxps://bzss[.]pt/cbb/
hxxps://marcioimoveis[.]pt/mit/
hxxps://bzss[.]pt/mail/
hxxps://sv-management[.]hospackfarma[.]nl/wix/verification[.]php
hxxps://guvenisi[.]com/js/cform/
hxxps://dynpyads[.]com/backup/
hxxps://canreisgroup[.]com[.]tr/backup/
hxxps://paixaobaptista[.]pt/data/
hxxps://sv-management[.]jetperformance[.]nl/wix/verification[.]php
hxxps://scmalmodovar[.]pt/mail/
hxxps://restaurantefialho[.]pt/mail/
hxxps://coureladozambujeiro[.]com/wp-mail/
hxxps://yuhz[.]confeciona[.]com/
hxxps://grupo-sk[.]com/mail/
hxxps://sv-management[.]firstresponder[.]nl/wix/verification[.]php
hxxps://mikro[.]pt/kund/
hxxps://weaving[.]pt/data/
hxxps://api[.]solarflevoland[.]nl/system_web/verification[.]php
hxxps://ccjc[.]pt/info/
hxxps://mr-bitcoin[.]ch/mail/
hxxps://aojdy5ex[.]dreamwp[.]com/wp-admin/css/colors/HOooo[.]php
hxxps://sv-management[.]solarflevoland[.]nl/wix/verification[.]php
hxxps://sv-weebly-manage[.]solarflevoland[.]nl/app/verification[.]php
hxxps://dpd-de[.]eyo-copter[.]com/pdpde/verification[.]php
hxxps://lp[.]washrocks[.]com/static/auth/en/verification[.]php
hxxps://ekademies[.]com/wp-mail/
hxxps://devwrapi[.]washrocks[.]com/home/verification[.]php
hxxps://gelalentejo[.]com/mail/
hxxps://devwrapi[.]washrocks[.]com/auth/en/verification[.]php
hxxps://faberkit[.]pt/Backup/
hxxps://luiscarmocx[.]com/Back/
hxxps://moqvk9zc[.]dreamwp[.]com/lo_gin/
hxxps://edificiomallorca[.]com/data/
hxxps://thewondersmx[.]com/mail/
hxxps://moqvk9zc[.]dreamwp[.]com/cr[.]php
hxxps://marketexpresso[.]site/admin/
hxxps://nookbees[.]com/mail/
hxxps://crazybubble[.]pt/data/
hxxps://vortica[.]net/mail/
hxxps://ytd[.]src[.]mybluehost[.]me/DPD/verification[.]php
hxxps://crazybubble[.]pt/mail/
hxxps://ateci[.]pt/Backup/
hxxps://creativetrendwatcher[.]be/mail/

hxxps://shf[.]com[.]pt/mail/
hxxps://candperdizes[.]com/mail/
hxxps://torvi[.]pt/Backup/
hxxps://raiugarts[.]com/mail/
hxxps://fhl[.]wvs[.]mybluehost[.]me/ch/anti/verification[.]php
hxxps://www[.]stassa[.]pt/wp-mail/
hxxps://aefpceup[.]pt/mail/
hxxps://bluesign[.]pt/kund/
hxxps://criamoda[.]com/mail/
hxxps://ald[.]azu[.]mybluehost[.]me/wp-content/ch/anti/verification[.]php
hxxps://blackcargo[.]pt/Backup/
hxxps://www[.]aeoj[.]org/mail/
hxxps://fixus[.]co[.]ao/mail/
hxxps://bluesign[.]pt/mail/
hxxps://carloscunhayoga[.]com/Backup/index[.]php
hxxps://carloscunhayoga[.]com/Backup/
hxxps://ilustremotivo[.]com/data/
hxxps://ilustremotivo[.]com/mail/
hxxps://gfc-angola[.]com/mail/
hxxps://crediadvisor[.]pt/inicio/
hxxps://uon[.]bow[.]mybluehost[.]me/DGT/verification[.]php
hxxps://sites-leiria[.]pt/financas/data/
hxxps://af-itsolutions[.]pt/mail/
hxxps://uon[.]bow[.]mybluehost[.]me/ch/verification[.]php
hxxps://scvidros[.]com[.]br/mail/
hxxps://sites-leiria[.]pt/es/
hxxps://ysu[.]ewp[.]mybluehost[.]me/sendgrid/verification[.]php
hxxps://graficateke[.]com[.]br/mail/
hxxps://www[.]autentifuturo[.]pt/mail/
hxxps://alojagora[.]com/mail/

Feel free to read other Sekoia.io TDR (Threat Detection & Research) analysis here:

CTI Cybercrime Infrastructure phishing