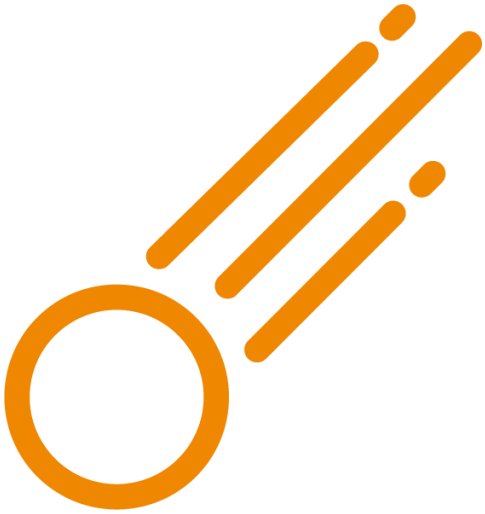


The Micro-Fraud Mechanism: Deconstructing Brazil's Gov.br and Pix Phishing Campaigns

Mario Lobo

Threat Intelligence Researcher at Lumu Technologies

Mauricio Ortega

Cyber Threat Intelligence Analyst at Lumu Technologies

The Pix-Fueled Scam Factory

Brazil is the largest economy in Latin America and one of the most advanced environments in the region regarding financial digitization and payment traceability. In November 2020, the Central Bank of Brazil (BCB) launched Pix: a pioneering instant payment ecosystem that currently processes transactions within seconds, 24/7, and free of charge for individuals, having achieved massive adoption across the adult population (Banco Central do Brasil, Relatório de Gestão do Pix).

This infrastructure coexists with the CPF (*Cadastro de Pessoas Físicas*), the unique tax identifier managed by the Receita Federal. Although its original purpose was strictly fiscal, the CPF mutated into a *de facto* universal identifier and frequently acts as a credential or primary authentication factor in **gov.br**, the centralized government services portal of the Brazilian state. This convergence transforms the CPF-Pix pairing into a critical vector for identity theft, government API exploitation, and automated financial fraud.

Lumu's CTI team has tracked a systematic campaign active for nearly a year, dedicated to impersonating Brazilian federal government entities. In this operation, threat actors weaponize public trust in official portals alongside the instant settlement of Pix through a dual monetization model: first, the harvesting and exfiltration of fiscal data for sale on the dark web and underground forums; second, the real-time collection of fictitious administrative fees via Pix for services that are never processed. This micro-fraud model marks an emerging tactical pivot in regional cybercrime: moving away from traditional high-value fraud attempts, operators now deliberately trade individual payout size for massive victim volume, bypassing automated antifraud alerts while scaling aggregate profits.

How the Scam Works

The attack scheme is straightforward. Although the CTI team has identified at least 3 distinct phishing kits targeting different entities, the attack lifecycle maintains a

© Lumu Technologies, Inc. All rights reserved.

consistent structure: the victim is directed to a phishing site impersonating **gov.br** portals, the Central Bank, or neobanks like Nubank or Will Bank, where a financial benefit is promised in their favor (either the refund of forgotten funds in the tax system or a pre-approved loan).

As an access control method, the attacker requests the victim's CPF. Upon capturing this identifier, the portal queries an automated personal data service that returns the victim's full name, date of birth, and mother's name. Armed with this context, the threat actor deploys distinct tactics to consolidate user trust:

- **On the government branch:** displays fake institutional videos, comments from alleged beneficiaries who have already withdrawn funds, and an interactive chat with audio explanations formulating questions to process the payout.
- **On the banking branch:** implements a pre-qualification form simulating credit analysis, approves it instantly, and displays a 10-minute countdown timer on screen to create urgency.

In both cases, to release the funds, the site demands payment of a supposed administrative/tax fee via Pix, immediately routing money directly into attacker-controlled accounts.

Hunting Beyond the Seed

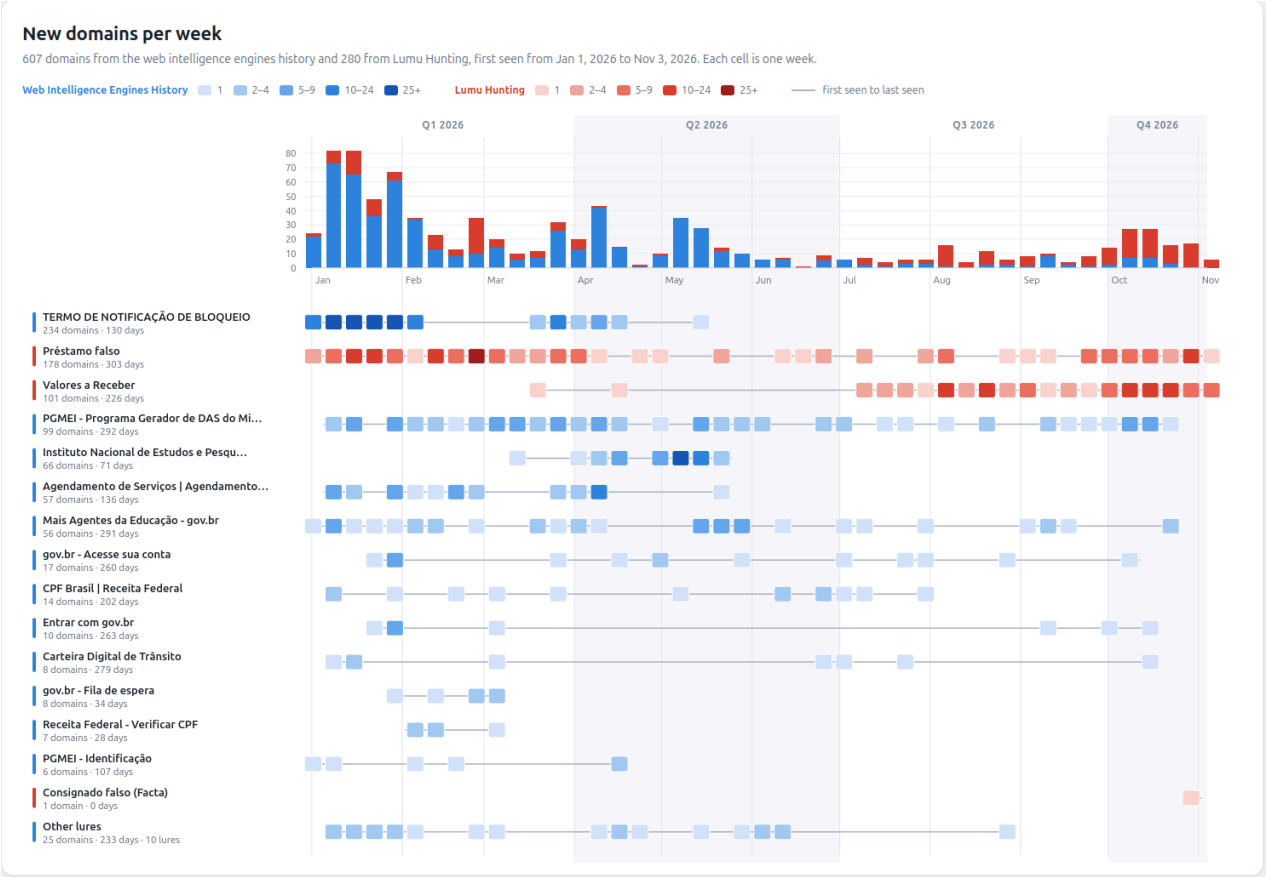
Throughout the current year, this behavior has consolidated, with hundreds of domains impersonating the Brazilian government using phishing lures such as Pix key blocking alerts, PGMEI (*Programa Gerador do DAS para o MEI*) fee collections, the Receita Federal, or generic websites with simulated gov.br logins. These findings cluster into three recurring kits tailored to different entities, all utilizing a landing page with CPF-based validation:

- **Fake loans:** impersonating banking entities and retailers.
- ***Sistema de Valores a Receber* (Unclaimed Funds):** Impersonating the institutional identity of Banco Central do Brasil.

© Lumu Technologies, Inc. All rights reserved.

- ***Crédito Consignado* (Fraudulent payroll-deducted loans):** under the name of Facta Financeira, a firm specializing in direct payroll or pension deduction loans.

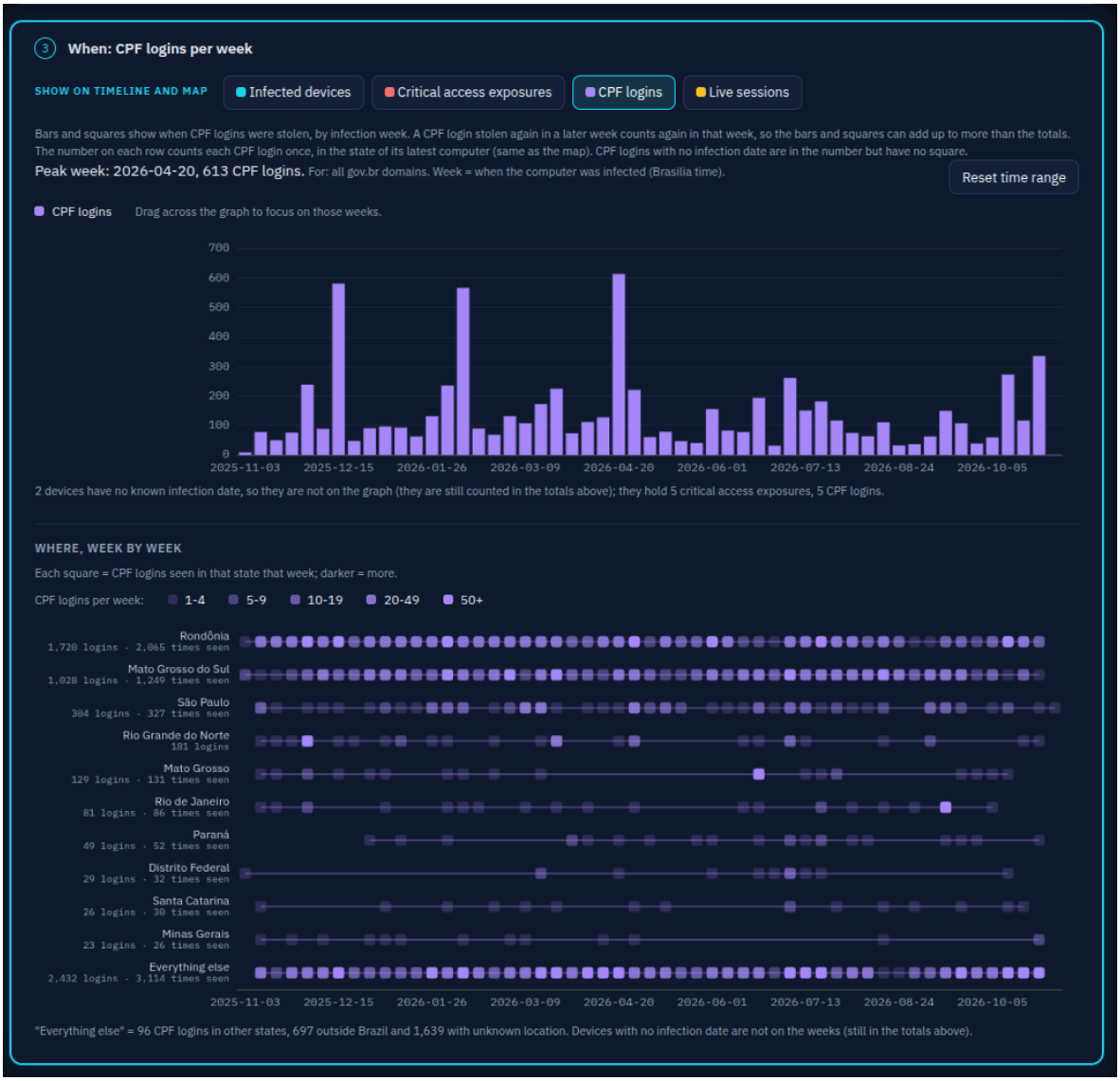
Lumu's CTI team tracked almost 900 domains linked to these campaigns throughout the year by combining historical web intelligence engine telemetry with proactive threat hunting. The detection gap regarding this activity widened significantly in the second half of the year: during Q3 and YTD Q4 2026, while conventional web intelligence engines recorded a cumulative historical total of 50 malicious domains, our proactive threat hunting identified 153 active domains, tripling visibility into the attacker's infrastructure.



Timeline: Above, weekly new domains, featuring historical web intelligence engines in blue and Lumu Hunting in red. Below, swimlanes by scam type, where each cell represents one week and the shading indicates the volume of newly observed domains.

© Lumu Technologies, Inc. All rights reserved.

This trend is also reflected in the rising volume of compromised CPF data in Brazil from late 2025 through 2026. These records correspond to accounts and portals where victims entered their CPF details, which were subsequently exfiltrated through diverse attack methods, including credential phishing and infostealer infections. A total of 6,002 compromised CPF account records identified for sale on the black market represents only the tip of the iceberg of these massive campaigns.



Geographic telemetry reveals that these compromises are heavily concentrated in specific Brazilian states, most notably São Paulo, Rondônia, and Mato Grosso do Sul.

© Lumu Technologies, Inc. All rights reserved.

While São Paulo reflects the sheer volume driven by its demographic and economic density, the elevated incidence in Rondônia and Mato Grosso do Sul highlights a disproportionate per capita impact across agricultural and frontier regions.

Inside the Kill Chain

To analyze how the scam operates internally, active domains were analyzed and the complete kill chain was documented for the two kits with the highest relevance due to their complexity and impact on victims. Below, we present first the analysis of the government branch, which concentrates the highest number of psychological manipulation tactics to gain user trust, followed by the commercial branch, utilizing Nubank as a case study for brand impersonation.

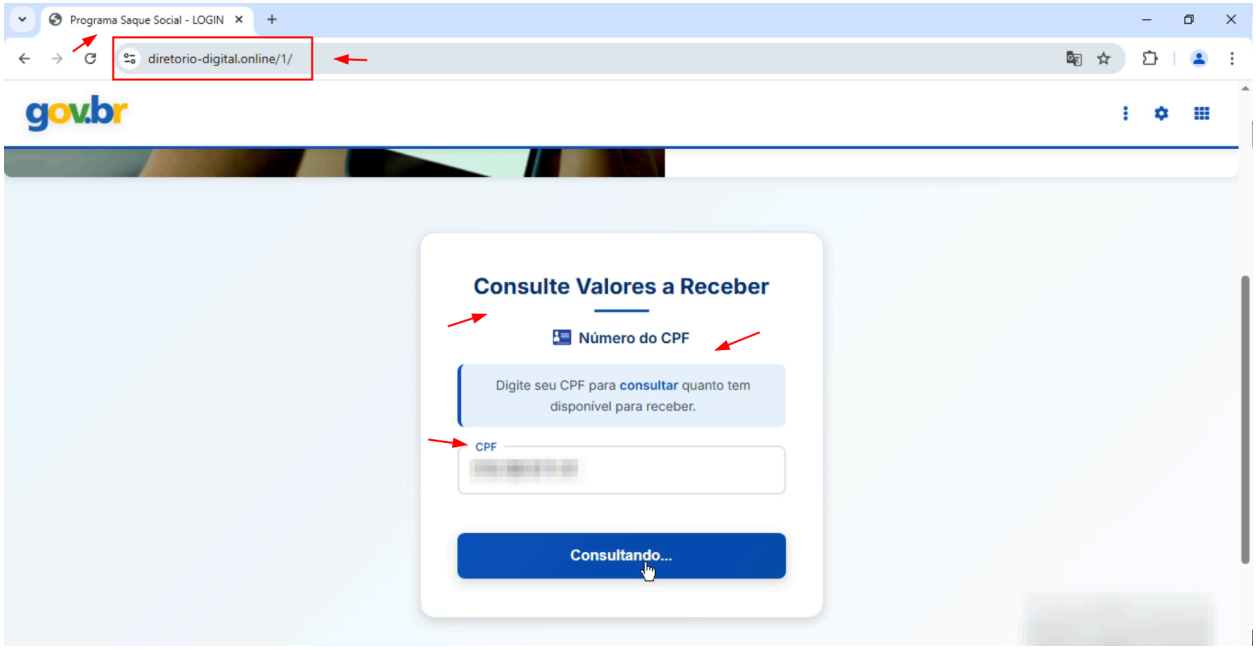
Government Branch: Sistema de Valores a Receber (SVR)

The attack chain initiates at **portaldoacesso[.]online**, a bridge page that redirects the victim to **diretorio-digital[.]online/1**, hosted on **64[.]23[.]238[.]59**. At this destination, the attacker impersonates Central Bank's SVR program using official gov.br visual branding. This phishing lure is exceptionally effective as it notifies users of unclaimed funds that they or a family member supposedly forgot in the financial system.

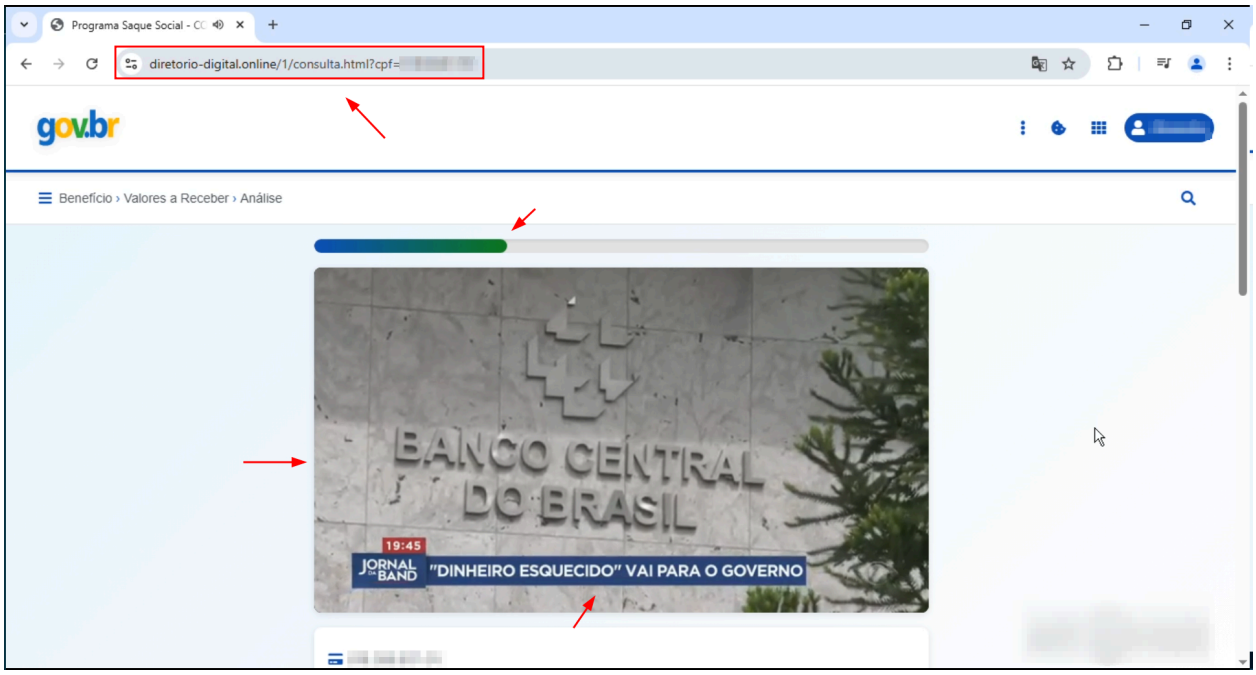
Following initial login, the site queries the CPF and displays videos alongside comments from fictitious beneficiaries claiming to have successfully retrieved their money. Subsequently, an interactive chat window opens featuring two instructional audio files promising a withdrawal of **R$ 5,960.50** (in the analyzed sample but amounts are similar in others). To release the payout, the platform demands a fictitious "*Saque Tax*" (Withdrawal Tax) of **R$ 86.63** via Pix, immediately diverting funds to the fraudster's account.

© Lumu Technologies, Inc. All rights reserved.

CPF lookup prompt.

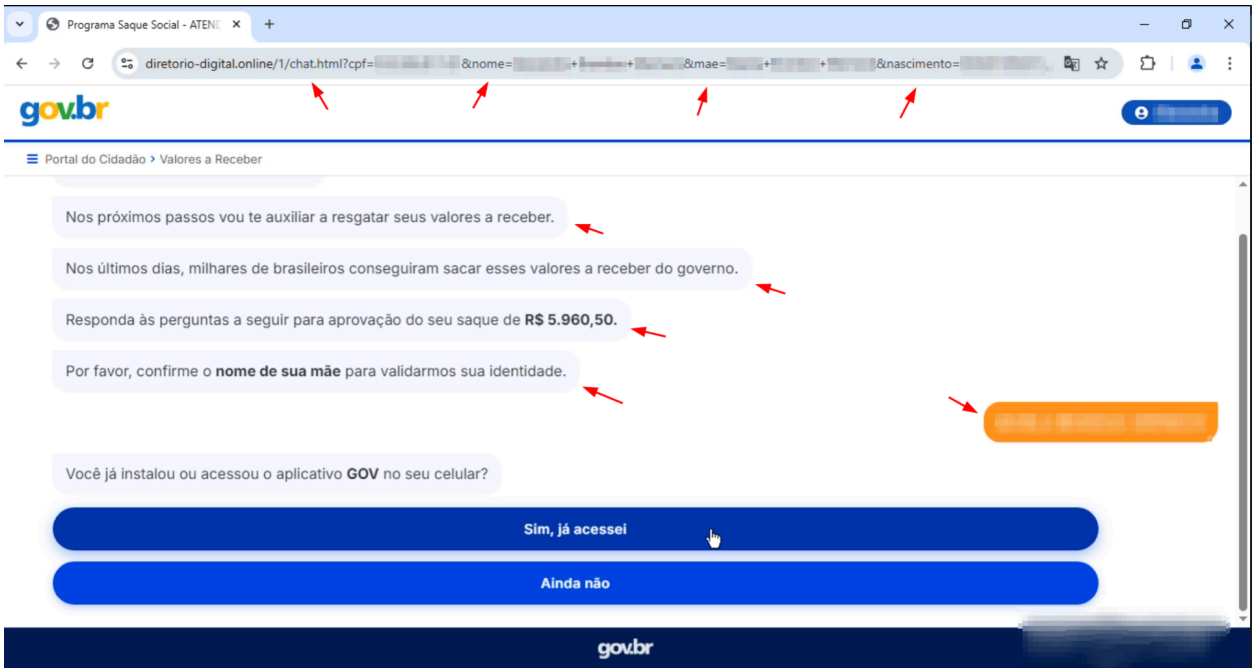


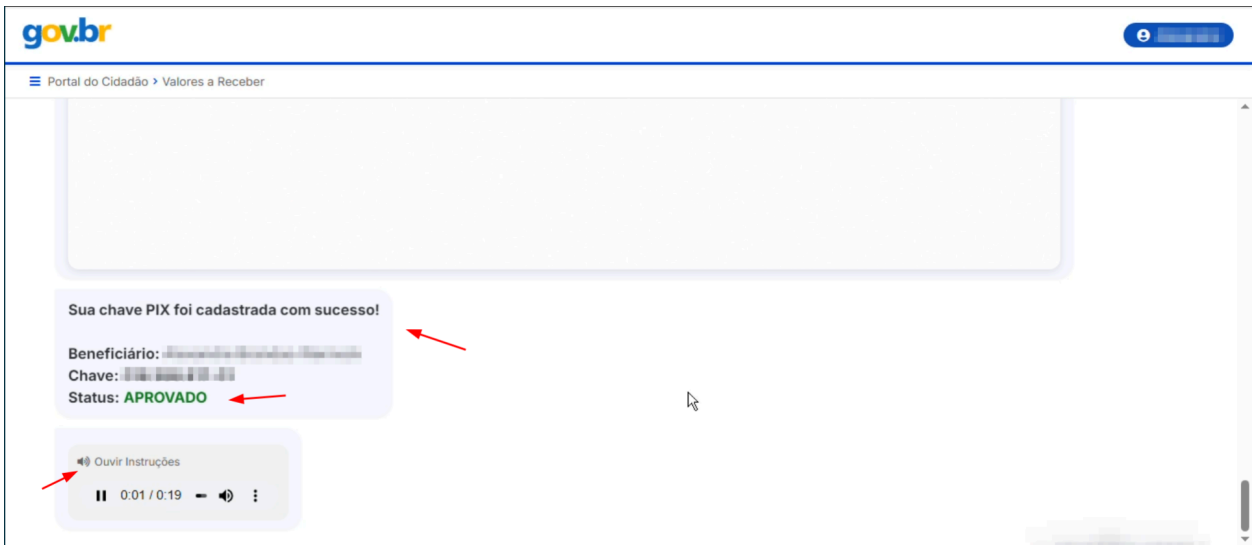
Video purportedly from the official "*Valores a Receber*" program warning that unclaimed money will revert to the government, paired with comments from alleged beneficiaries to build trust and urgency.



© Lumu Technologies, Inc. All rights reserved.

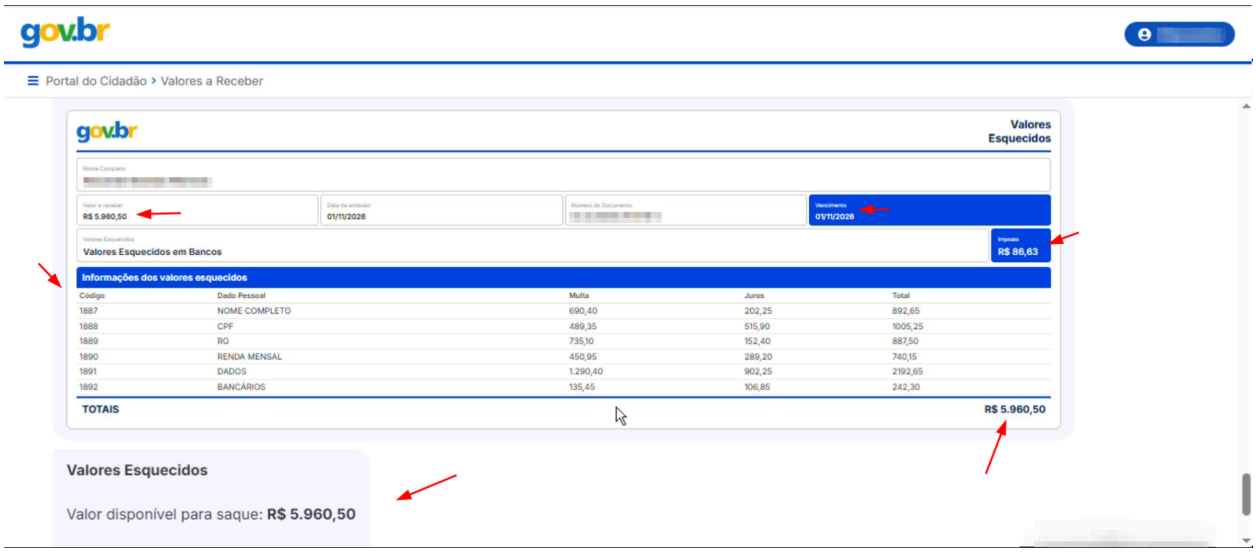
The scam system launches a chat requesting the victim to confirm their mother's name and answer identity validation and financial questions, delivering audio instructions after each approval step.

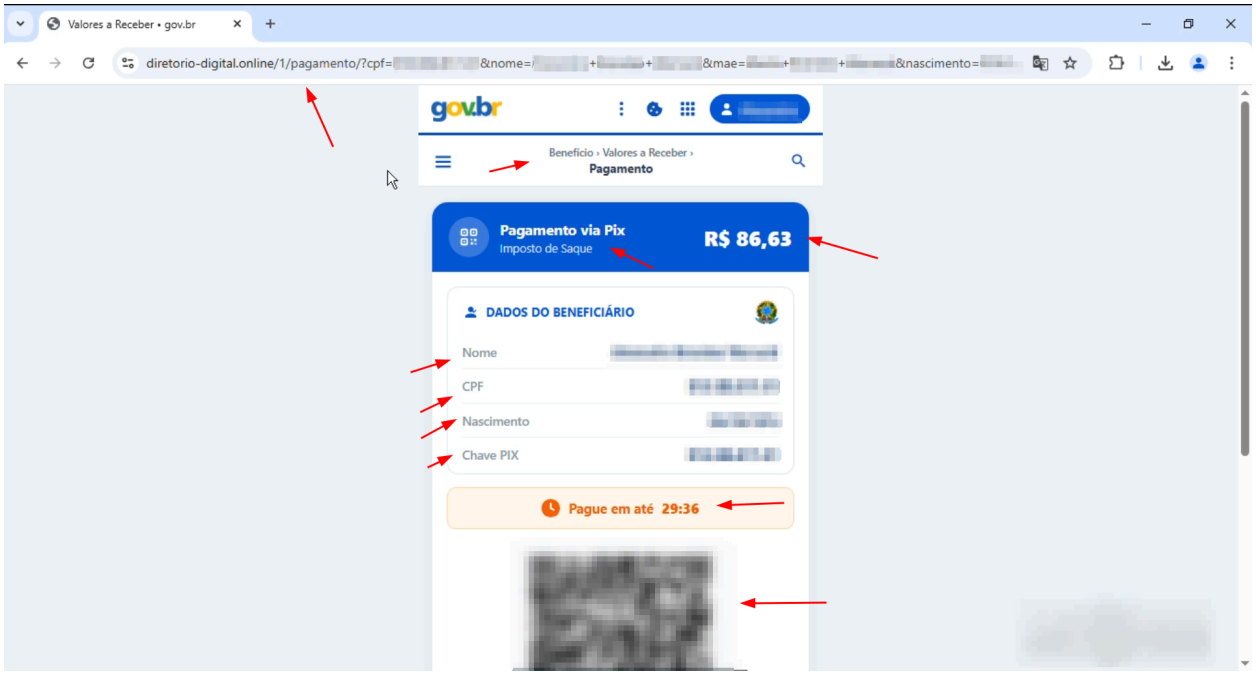




© Lumu Technologies, Inc. All rights reserved.

The fraudulent page generates a fake official withdrawal receipt, explaining why the victim must pay a refundable fee, displaying the Pix QR code for collection.





© Lumu Technologies, Inc. All rights reserved.

Financial Branch: Nubank

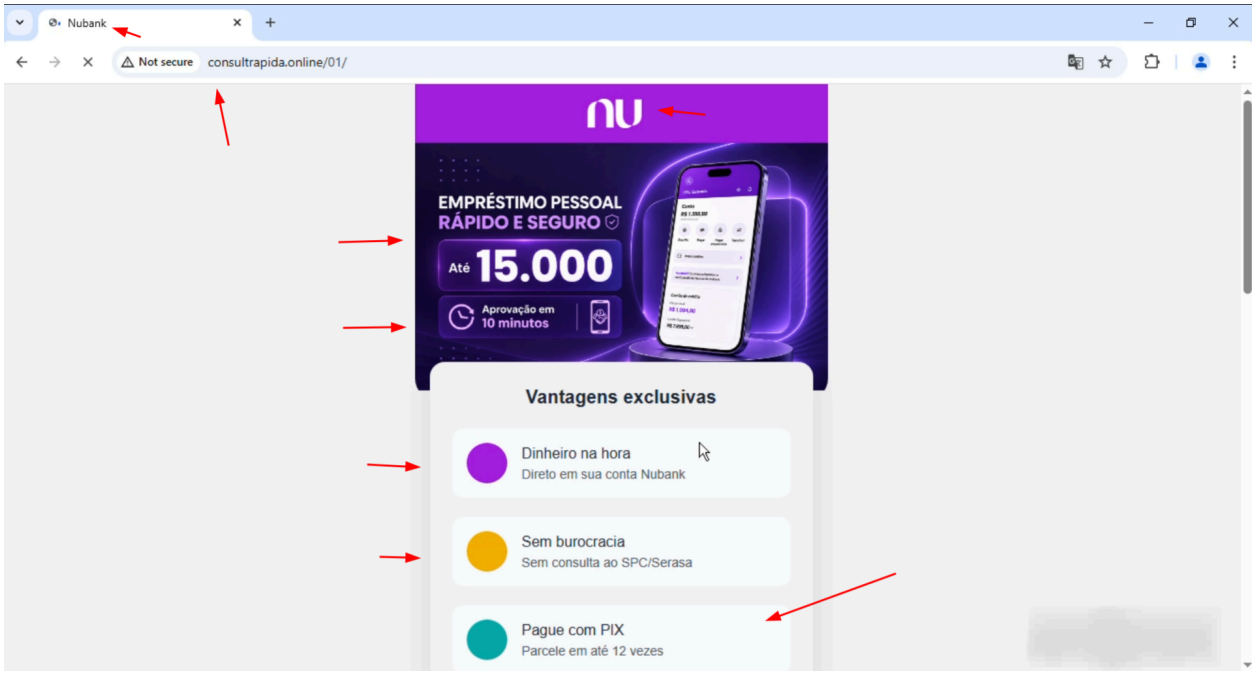
On the commercial branch, the domain **consultrapida[.]online,** hosted on **192[.]185[.]211[.]243**, served as a case study. In this scenario, the phishing lure exploits the Nubank brand identity to offer fraudulent pre-approved loans. Adhering to the campaign-wide pattern, the site first requests the victim's CPF to validate and enrich the session context. Next, it displays a dynamic pre-analysis questionnaire to simulate credit evaluation and issue immediate fake approval.

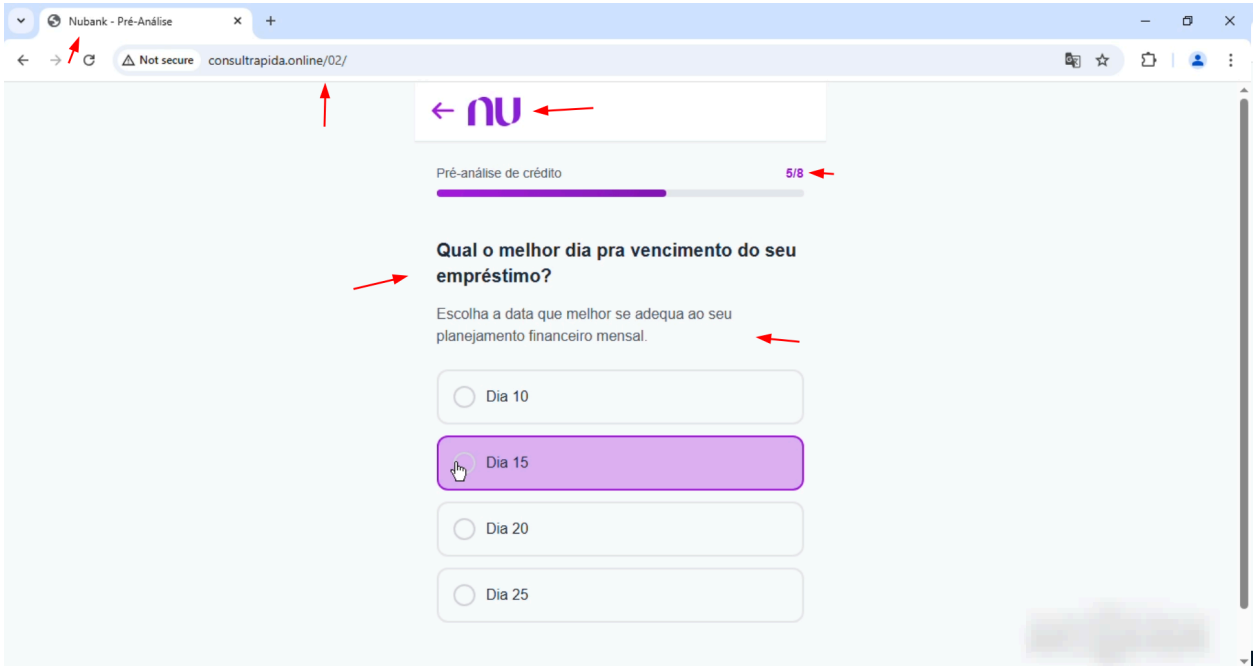
During the monetization phase, the kit notifies an administrative fee of **R$ 28.63** to disburse the loan. However, upon redirecting to the checkout gateway, an operational inconsistency across these deployments emerges: the final amount settled via Pix is **R$ 28.93**, a fee discrepancy likely stemming from template desynchronization or automatic gateway surcharges applied by the cybercriminal's intermediary payment processor.

Analysis of this transaction revealed a critical nexus: the payment shares the exact same registered recipient as the government branch, identified under the truncated business name "***PLITUNI INTERMEDIACAO DE***". This overlap strongly supports the hypothesis of a single threat actor (or unified operation) managing monetization infrastructure across both lure themes.

Furthermore, across both campaign branches, the Pix code generation chain points to the subdomain **qrcode.fyhub[.]com[.]br**, the payment orchestration platform responsible for generating dynamic checkout codes.

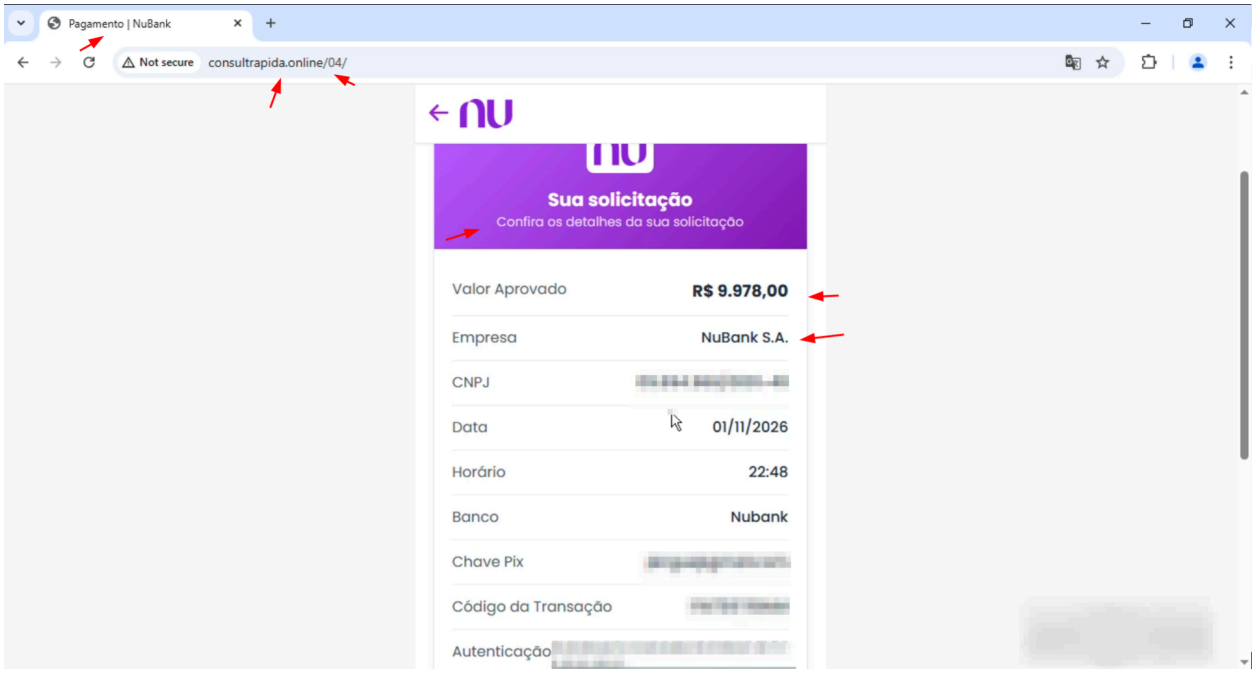
© Lumu Technologies, Inc. All rights reserved.



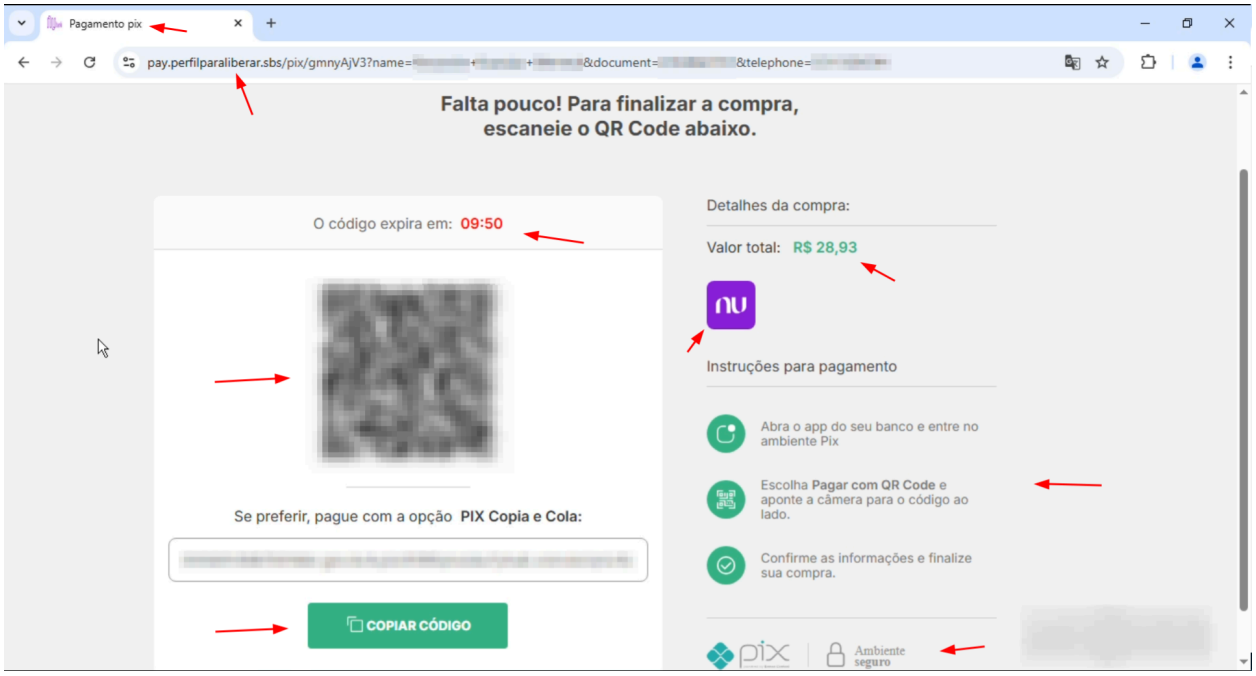


Landing page impersonating Nubank offering loans up to **R$ 15,000**, 10-minute approval, and no credit bureau (SPC/Serasa) check. Followed by a fake credit pre-analysis questionnaire simulating victim evaluation.

© Lumu Technologies, Inc. All rights reserved.



The page displays confirmation of an approved loan for **R$ 9,978.00**. After ~4 minutes of deliberate delay designed to simulate administrative processing, it imposes a 10-minute window to pay the fee and redirects to a checkout charging **R$ 28.93** via Pix with a code that expires after a short time period.



© Lumu Technologies, Inc. All rights reserved.

Conclusions

- **Unified Infrastructure and Attribution:** The evidence documented in this investigation confirms that the three analyzed kits converge across key stages of both hosting infrastructure and monetization points (sharing the same beneficiary and Pix QR code endpoints). This technical overlap supports the hypothesis of a single threat actor, or a small, coordinated criminal cluster, operating this architecture in a continuous and systematic flow.
- **Low-Impact, High-Volume Operating Model:** The scheme replaces traditional high-value financial fraud with a granular monetization strategy (*low-and-slow*): the mass extraction of micro-payments (ranging between R$ 28 and R$ 86). Because these amounts are minimal, the attack reduces the victim's psychological friction to authorize the payment, remains below the alert thresholds of banking anti-fraud engines, and discourages victims from filing formal reports with law enforcement.
- **Attack Surface and Persistence:** By exploiting the CPF as a digital identity key and leveraging the irreversible immediacy of Pix, this vector establishes itself as one of the most scalable, automated, and elusive social engineering operations within the Brazilian cybercrime ecosystem.
- **Lumu's Proactive Hunting and Telemetry Advantage:** The significant visibility gap documented in this investigation, where Lumu uncovered 153 malicious domains compared to just 50 cataloged by traditional web intelligence engines for Q4, underscores the critical necessity of proactive threat hunting over reactive monitoring. Organizations operating in Brazil and regional customers leverage this asymmetrical advantage directly through Lumu's proprietary internal data feeds. By continuously analyzing network metadata and correlating shared monetization infrastructure in real time, Lumu delivers exclusive, early-stage intelligence, enabling security teams to preemptively block fraudulent campaigns before public disclosure and mitigate exposure well before threat actors achieve widespread scale.

© Lumu Technologies, Inc. All rights reserved.

ATT&CK

6 techniques across 4 tactics. Enterprise Matrix, ATT&CK v20.0.
Shared folder: mitre_attack_cpf_scam_brazil_en[.]xlsx

IoCs

We provide the 153 domains identified during Q3 and YTD Q4 2026 representing the most recent activity of this cybercriminal operation. Domains identified in previous quarters are preserved for historical research tracking.

None

```
portaldoacesso[.]online
diretorio-digital[.]online
consultrapida[.]online
acessecaxseguro[.]online
acessoportaldigital[.]com
ajudanasinfmis[.]site
ambienteseguro[.]xyz
atendimento1[.]pages[.]dev
atendimentorapido[.]space
attt3ndmnto[.]quest
blognovidadesbrasil[.]lat
caixahoje[.]online
centraldeacessobrcax[.]com
centraldeanalisevalores[.]shop
centralgoldnu[.]fun
centralvipdigital[.]online
certificadocredito[.]site
certodimeno[.]site
confirasuasopcoes[.]site
consulta-valoresareceber[.]sbs
consulta5[.]dreamhosters[.]com
consultafacil2026[.]vercel[.]app
consultaoficial04[.]dreamhosters[.]com
consultaonline[.]shop
consultaonline2[.]dreamhosters[.]com
consultaprontacaxbr[.]com
```

© Lumu Technologies, Inc. All rights reserved.

consultarapidaonline[.]store
consultarliberacao[.]online
consultasaldosbr[.]shop
consultaseusvalores[.]lat
consultaseusvalores[.]space
consultaseusvalores[.]website
consultasimples[.]store
consulteagoraonline[.]com
consulteagr[.]netlify[.]app
consulterapidoagora[.]lol
consulterapidoagora[.]space
consultesuasopcoes[.]com
consultsecundaria[.]shop
consultssald[.]online
creditoagil[.]cfd
desenrolaagora[.]lol
disponivelcredito[.]online
entendasuaconsulta[.]monster
escritoinfo[.]site
factrafinanceira[.]tech
financerorapido[.]fun
fiquelimpodes2026[.]digital
fonsecadias731[.]workers[.]dev
formularioconsulta2026[.]click
gov-nine-zeta[.]vercel[.]app
ideniza-brasil[.]vercel[.]app
iinfsbrsill[.]site
indeniza-bcb[.]vercel[.]app
indenizaminhacbbr[.]vercel[.]app
infobasicbox[.]site
infoboxzero[.]site
infopowrin[.]site
informandoseagora[.]online
informesws[.]fun
infotecbr[.]online
liberar-valores[.]com
mansierto[.]site
monseimo[.]site
monsiimo[.]site
mosemise[.]site

© Lumu Technologies, Inc. All rights reserved.

```
mymixz[.]online
noticiandoaqui[.]online
novonuappbank[.]com
novonuappbanks[.]shop
nowinfobs[.]store
nubconsul[.]online
nucompleto-dev[.]pages[.]dev
ofertadehoj[.]online
onlineconsultacredito[.]online
onlineconsultarapida[.]online
organizasuavidafinanceira[.]site
pagarmesegurocax[.]online
paginaoficial[.]site
pesquisavaloresconecta[.]shop
pontodeacessocaxbr[.]com
portal-seguro-3390[.]vercel[.]app
portalacessooficial[.]site
portalconsultacax[.]online
portalconsultavalors[.]online
portaldevalores[.]online
pportalsaibamaisclientes[.]online
processoanaliseonline[.]site
processodeavaliacaodigital[.]site
processodeconsultabronline[.]site
processodeconsultabrtech[.]site
produzindoconteudo[.]xyz
programa04[.]online
propostaverificadaoficial[.]site
prospera-mei[.]netlify[.]app
reidoburgao[.]delivery
resgatwebonline[.]pages[.]dev
roxinho-velani-2-0[.]pages[.]dev
runpage[.]dev
saaminoms[.]site
saaminomsa[.]site
seuvaloragorabrasil[.]vercel[.]app
seuvaloroficial[.]vercel[.]app
seuvalrareceber[.]com
simlasfable[.]net
somindemin[.]site
```

© Lumu Technologies, Inc. All rights reserved.

```
ssoriobrsyll[.]site
suaanaliseagora[.]com
suaconsulta-rapida[.]online
suasopcoesdisponiveis[.]site
suasopcoesonline[.]site
supercredito[.]site
supercredito[.]store
suportedigitalbr[.]xyz
valorees[.]pages[.]dev
valores-5cu[.]pages[.]dev
valoresareceber-bcb-br[.]site
valoresareceber-bcb-br[.]vercel[.]app
valoresareceber-bcbb-br[.]vercel[.]app
valoresareceber[.]sbs
valoresareceberbcbcentraldados[.]com
valoresareceberbcbcentralinfo[.]com
valoresareceberbcbconsultabr[.]com
valoresareceberbcbconsultadigital[.]com
valoresareceberbcbconsultafacil[.]com
valoresareceberbcbconsultas[.]com
valoresareceberbcbguiaweb[.]com
valoresareceberbcbinformacoes[.]com
valoresareceberbcbonline[.]com
valoresareceberbcborientacoes[.]com
valoresareceberbcbpainelweb[.]com
valoresareceberbcbpesquisabr[.]com
valoresareceberbcbseguro[.]com
valoresareceberbcbverificacaoonline[.]com
valoresarecebergov-meusaldott[.]vercel[.]app
valoresareceberr-bcb-br[.]vercel[.]app
valoresarecieber-bcb[.]shop
valoress[.]xyz
verificacaodevalores[.]online
verificacaolistcaxbr[.]online
verificadoaqui[.]online
verificadobem[.]online
verificadohoje[.]online
verificadomeu[.]online
verificadomkt[.]online
verificandoinformacoes[.]beauty
```

© Lumu Technologies, Inc. All rights reserved.

```
verifiqlistcaix[.]online
webdigitalacesso[.]online
withixt[.]online
wokkpit[.]space
woraaakp[.]click
workppscel[.]click
workspacenetwork[.]online
```

© Lumu Technologies, Inc. All rights reserved.