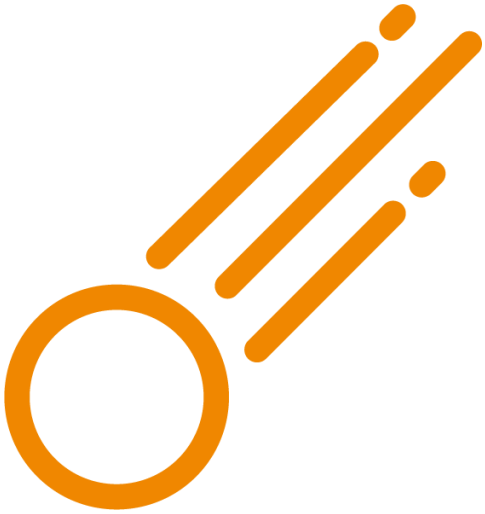


# O Mecanismo de Microfraude:
# Desconstruindo as Campanhas de Phishing contra o Gov.br e o Pix


**Mario Lobo**

Threat Intelligence Researcher at Lumu Technologies

**Mauricio Ortega**

Cyber Threat Intelligence Analyst at Lumu Technologies

# A Fábrica de Golpes que Vive do Pix

O Brasil é a maior economia da América Latina e um dos ambientes mais avançados da região em digitalização financeira e rastreabilidade de pagamentos. Em novembro de 2020, o Banco Central do Brasil (BCB) lançou o Pix: um ecossistema de pagamentos instantâneos pioneiro que hoje processa transações em segundos, 24/7 e sem custo para pessoas físicas, adotado de forma massiva pela população adulta (Banco Central do Brasil, Relatório de Gestão do Pix).

Essa infraestrutura convive com o CPF (*Cadastro de Pessoas Físicas*), o identificador tributário unívoco administrado pela Receita Federal. Embora seu propósito original fosse estritamente fiscal, o CPF mutou para um identificador universal *de facto* e atua com frequência como credencial ou fator primário de autenticação no **gov.br**, o portal centralizado de serviços do Governo Federal brasileiro. Essa convergência transforma o binômio CPF-Pix em um vetor crítico para roubo de identidade, exploração de APIs governamentais e fraude financeira automatizada.

A equipe de CTI (*Cyber Threat Intelligence*) da Lumu documentou uma campanha sistemática ativa há quase um ano, dedicada a suplantar entidades do governo federal brasileiro. Nesta operação, os atores de ameaça instrumentalizam a confiança pública nos portais oficiais combinada à liquidação instantânea do Pix por meio de um modelo de monetização dupla: primeiro, a coleta e exfiltração de dados fiscais para venda na dark web e em fóruns clandestinos; segundo, a cobrança fraudulenta em tempo real de taxas administrativas fictícias via Pix por serviços que nunca chegam a ser processados. Esse modelo de micro-fraude marca uma mudança tática emergente no cibercrime regional: afastando-se dos fraudes tradicionais de valores elevados, os operadores agora trocam deliberadamente a quantia de cada golpe por um volume massivo de vítimas, contornando alertas automatizados dos sistemas antifraude enquanto escalam os lucros acumulados.

© Lumu Technologies, Inc. All rights reserved.

# Como Funciona o Golpe

O esquema da fraude é direto. Embora a equipe de CTI tenha identificado pelo menos 3 *kits* de phishing voltados a diferentes entidades, o ciclo de ataque mantém sempre a mesma estrutura: a vítima é direcionada a um site falso que suplanta portais do **gov.br**, do Banco Central ou de neobancos como Nubank ou Will Bank, onde se promete um benefício financeiro a seu favor (seja a devolução de valores esquecidos no sistema financeiro ou um crédito pré-aprovado).

Como método de acesso e engajamento inicial, o atacante solicita o CPF. Após capturar esse identificador, o portal consulta um serviço automatizado de enriquecimento de dados pessoais que retorna o nome completo da vítima, sua data de nascimento e o nome da mãe. Com essas informações, o ator de ameaça desdobra distintas táticas de engenharia social para consolidar a confiança da vítima:

- **Na vertente governamental:** projeta vídeos institucionais falsos, comentários de supostos beneficiários que já teriam sacado o dinheiro e um chat interativo com áudios explicativos que formulam perguntas para processar o resgate.
- **Na vertente bancária:** implementa um formulário de pré-qualificação que simula a análise de crédito, aprova-o imediatamente e impõe um contador regressivo de 10 minutos na tela para pressionar o usuário.

Em ambos os casos, para liberar os recursos, o site exige o pagamento de uma suposta taxa administrativa/tarifa via Pix, canalizando o dinheiro de forma instantânea para contas sob o controle dos Cibercriminosos.

© Lumu Technologies, Inc. All rights reserved.

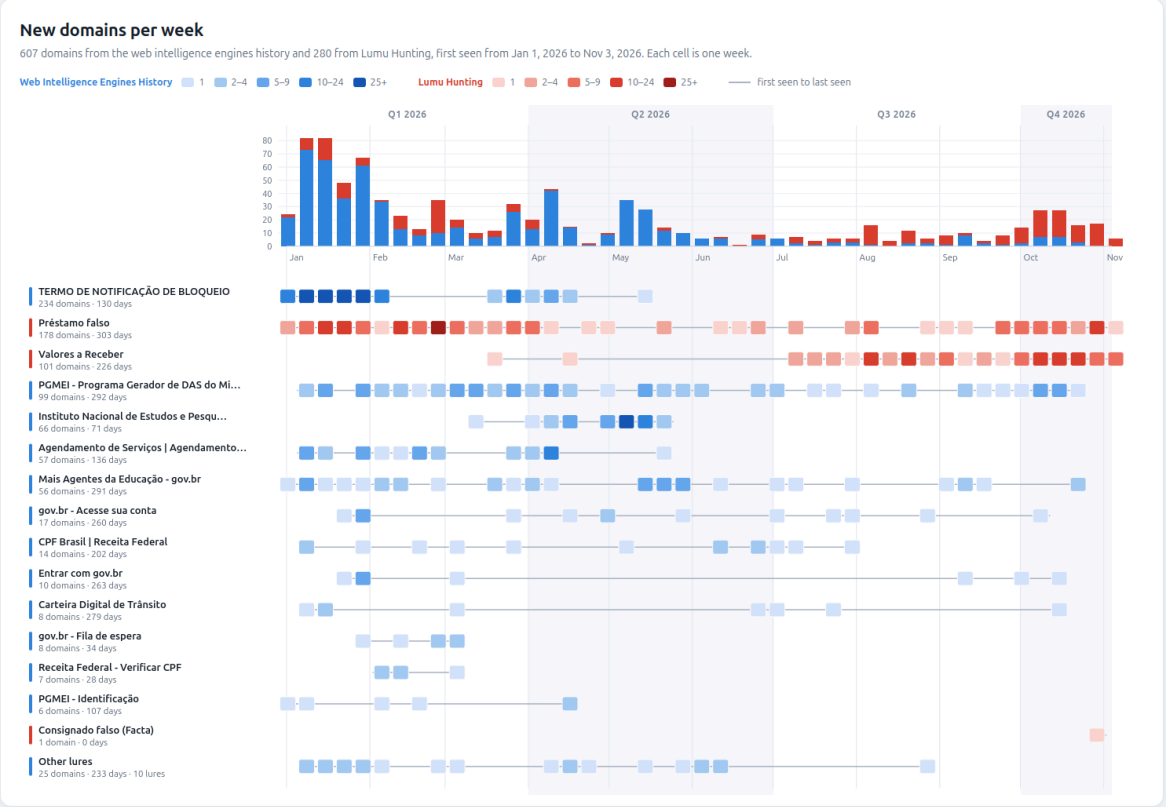
# Hunting Além da Semente (Beyond the Seed)

Ao longo do ano, esse comportamento se consolidou com centenas de domínios suplantando o governo brasileiro por meio de iscas como o bloqueio de chaves Pix, cobranças do PGMEI (*Programa Gerador do DAS para o MEI*), a Receita Federal ou sites genéricos com login simulado do gov.br. Nossas descobertas podem ser agrupadas em três categorias de *kits* recorrentes adaptados a distintas entidades, os quais empregam uma landing page com validação via CPF:

- **Empréstimos falsos:** suplantando entidades bancárias e comércios.
- **Valores a Receber:** usurpando a identidade visual do Banco Central do Brasil.
- **Crédito consignado fraudulento:** em nome da Facta Financeira, firma especializada em empréstimos com desconto em folha/benefício.

A equipe de CTI da Lumu rastreou quase 900 domínios vinculados a essas campanhas ao longo do ano, misturando a análise histórica de motores de inteligência web com exercícios próprios de threat hunting. A lacuna na capacidade de detecção frente a esse comportamento é contundente no segundo semestre do ano: durante o Q3 e o decorrer do Q4 de 2026, enquanto os motores convencionais de inteligência web registraram um acumulado histórico de 50 domínios maliciosos, nossa caça proativa de ameaças identificou 153 ativos, triplicando a visibilidade sobre a infraestrutura do atacante.

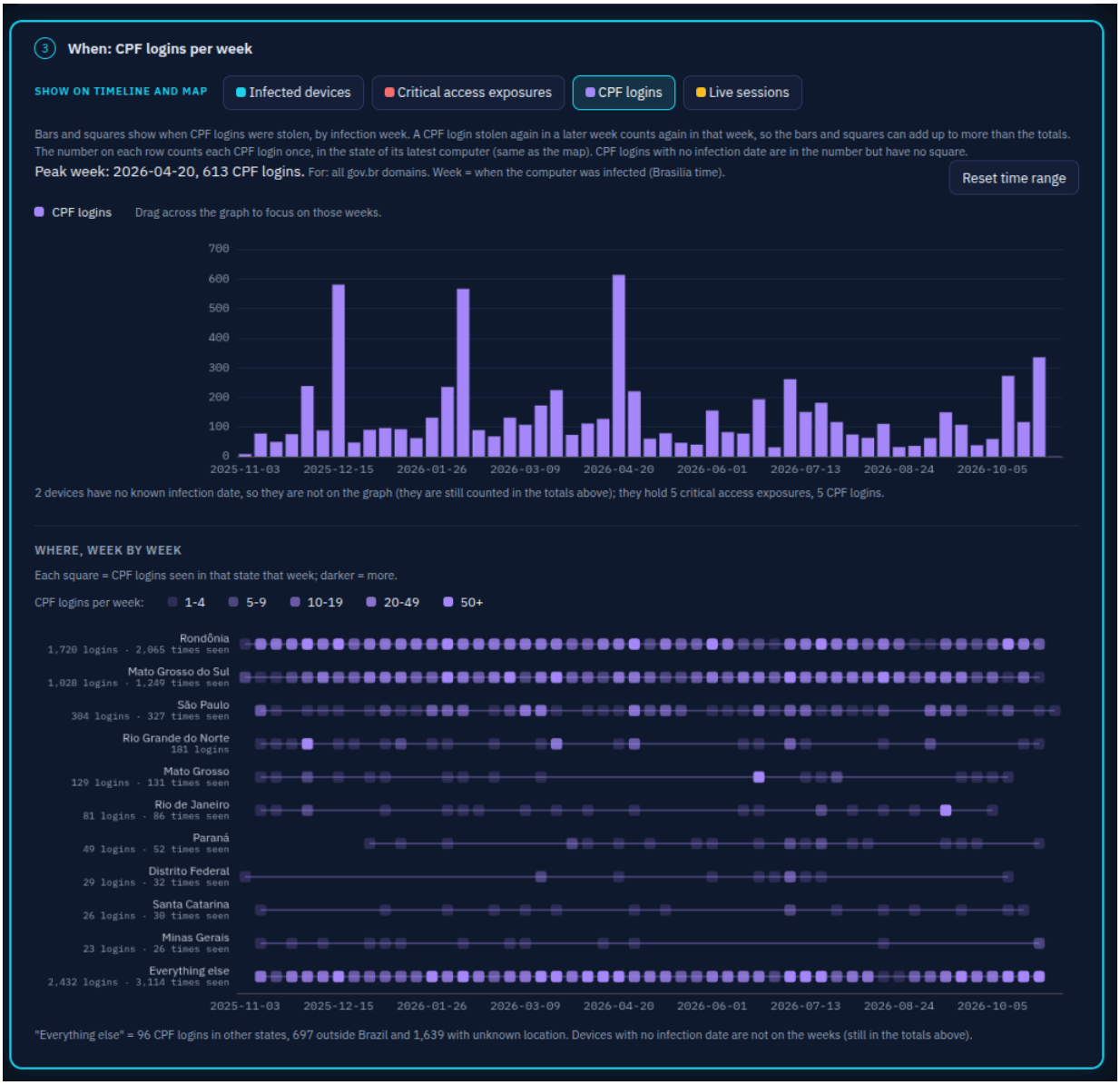
© Lumu Technologies, Inc. All rights reserved.




**Linha do Tempo:** os domínios novos criados a cada semana demonstram a evolução contínua da infraestrutura maliciosa operada pelos cibercriminosos.

Essa tendência também se reflete no volume crescente de dados de CPFs comprometidos no Brasil entre o final de 2025 e 2026. Esses registros correspondem a contas e portais em que as vítimas inseriram suas credenciais de CPF, posteriormente exfiltradas por múltiplos vetores de ataque, incluindo *phishing* de credenciais e infecções por *infostealers*. O total de 6.002 registros de contas com CPFs comprometidos identificados à venda em fóruns clandestinos representa apenas a ponta do *iceberg* diante da escala dessas campanhas massivas.

© Lumu Technologies, Inc. All rights reserved.




Em termos geográficos, a telemetria revela uma concentração acentuada desses comprometimentos em estados como Rondônia, Mato Grosso do Sul e São Paulo. Enquanto São Paulo reflete o volume absoluto decorrente de sua densidade econômica e populacional, os índices expressivos em Rondônia e no Mato Grosso do Sul chamam a atenção por um impacto desproporcional em termos *per capita*.

© Lumu Technologies, Inc. All rights reserved.

# Por Dentro da Kill Chain

Para entender como a fraude opera em detalhes técnicos, analisamos os domínios ativos e documentamos a *kill chain* completa dos dois *kits* com maior relevância por sua complexidade e impacto. A seguir, apresenta-se o estudo da vertente governamental e, posteriormente, a vertente comercial, utilizando o Nubank como exemplo de marca suplantada.

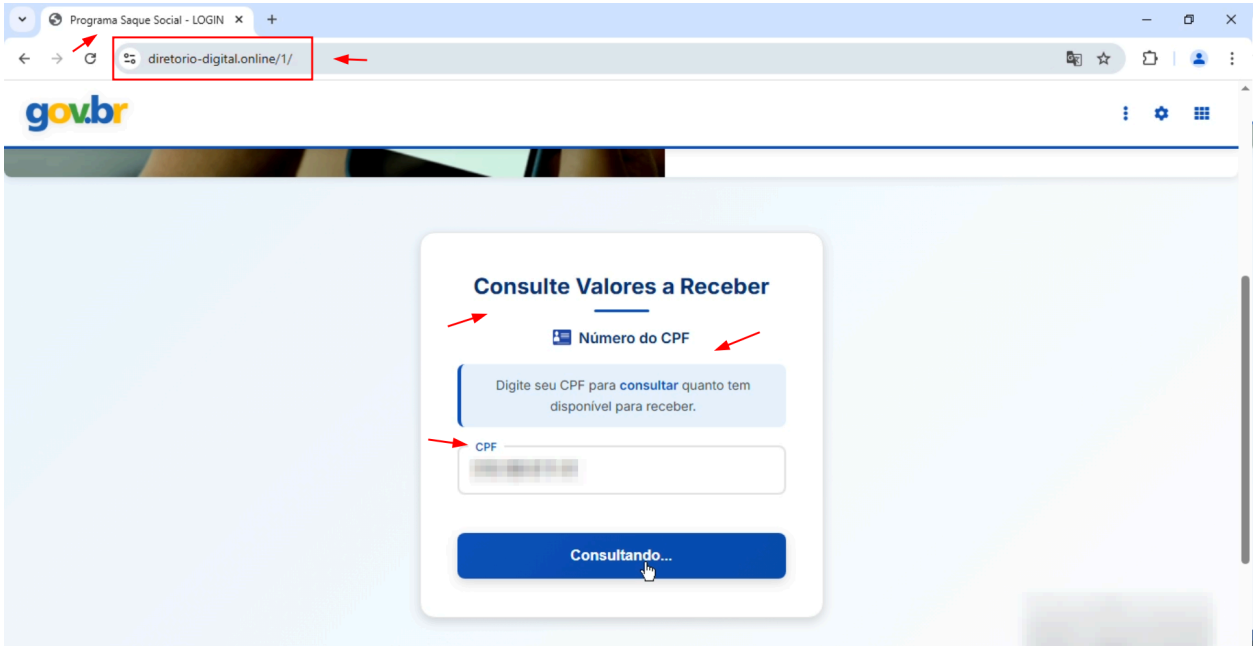
## Vertente Governamental: Sistema de Valores a Receber (SVR)

A cadeia de ataque inicia em **portaldoacesso[.]online**, uma página de redirecionamento (*landing page/bridge*) que envia a vítima para **diretorio-digital[.]online/1**, recurso hospedado no IP **64[.]23[.]238[.]59**. Nesse destino, o atacante suplanta o programa SVR do Banco Central sob a identidade visual do **gov.br**. Esse programa é especialmente atraente ao notificar sobre montantes que o usuário ou algum familiar supostamente esqueceram de resgatar no sistema financeiro.

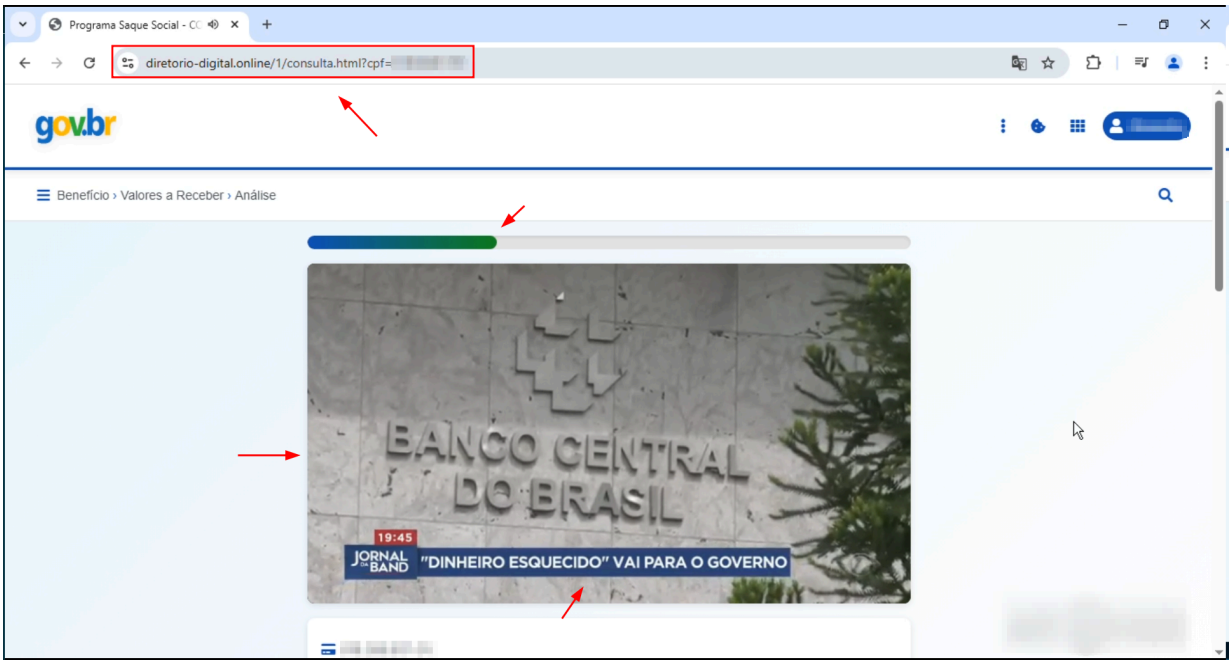
Após o suposto início de sessão, o site consulta o CPF e exibe vídeos com comentários de supostos beneficiários afirmando ter cobrado seus valores. Em seguida, abre-se uma janela de chat interativo com dois áudios de instruções onde se promete um resgate de **R$ 5.960,50** (no caso analisado mas os valores em outros casos são similares). Para liberar o valor, a plataforma cobra um suposto "Imposto de Saque" de **R$ 86,63** via Pix, desviando os fundos imediatamente para a conta do estafador.

© Lumu Technologies, Inc. All rights reserved.

Consulta do CPF.

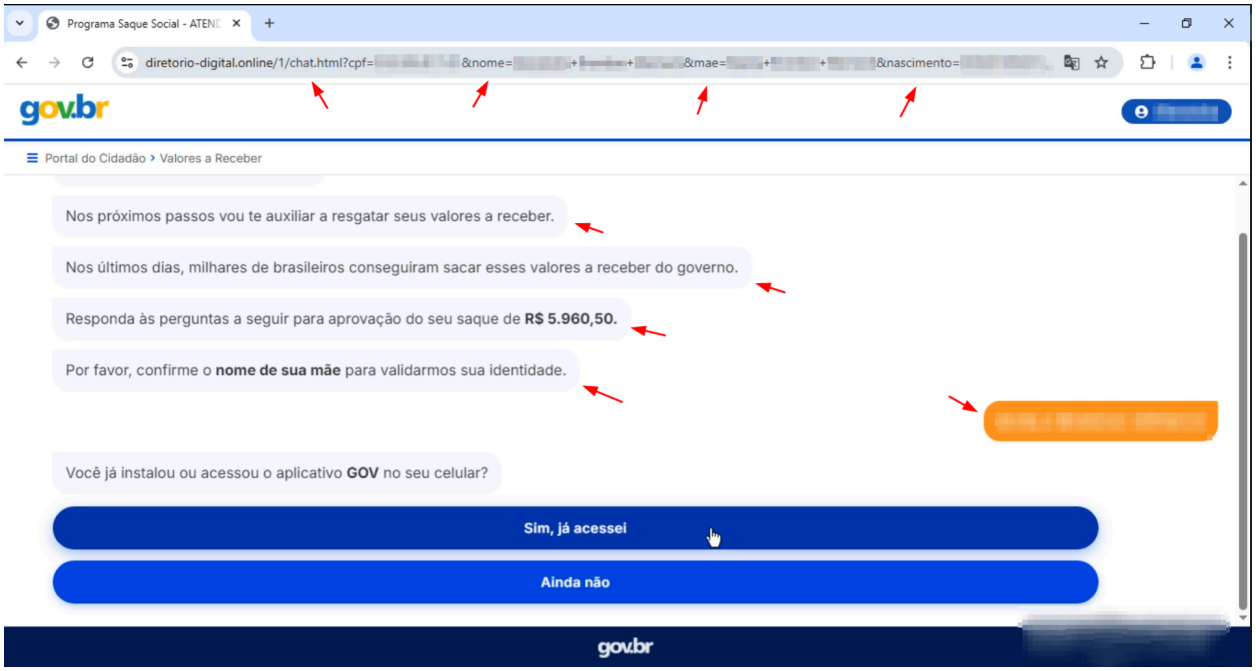


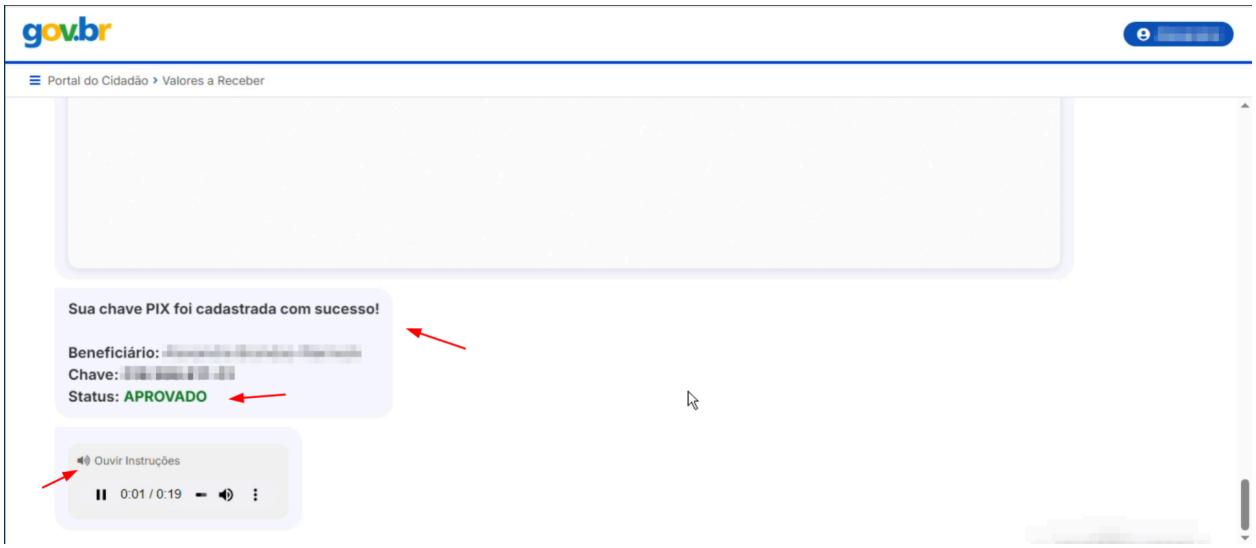

Vídeo aparentemente oficial do programa «Valores a Receber», que alerta que o dinheiro não reclamado ficará com o governo, acompanhado de comentários de supostos beneficiários para gerar confiança e urgência.




© Lumu Technologies, Inc. All rights reserved.

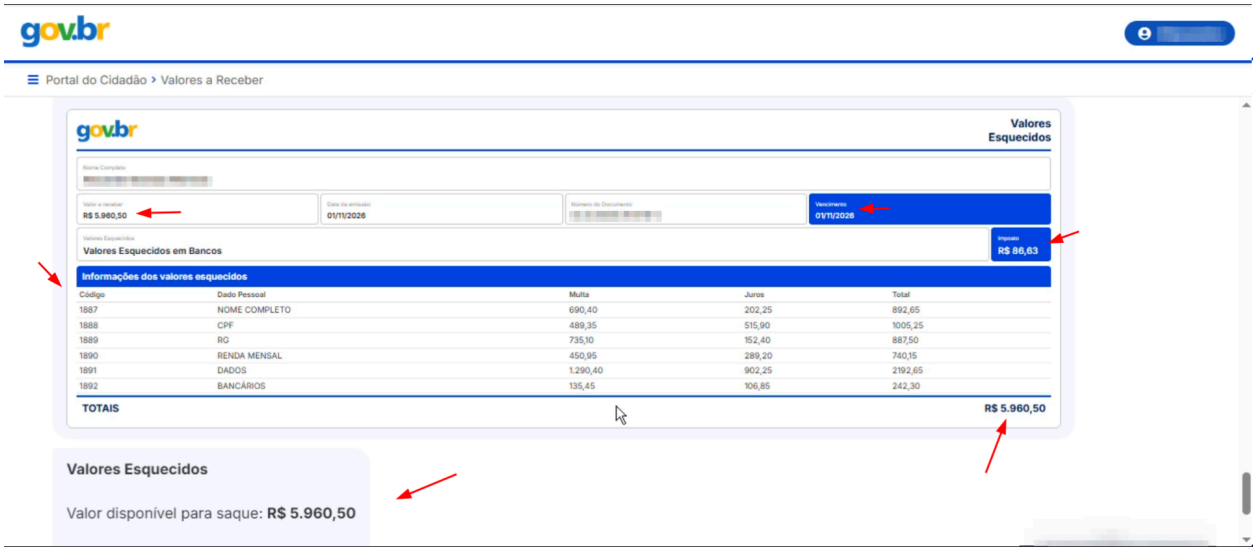
O sistema do fraude inicia um chat que solicita à vítima confirmar o nome da mãe e responder a perguntas de validação de identidade e informações financeiras, além de enviar um áudio com instruções após cada aprovação.

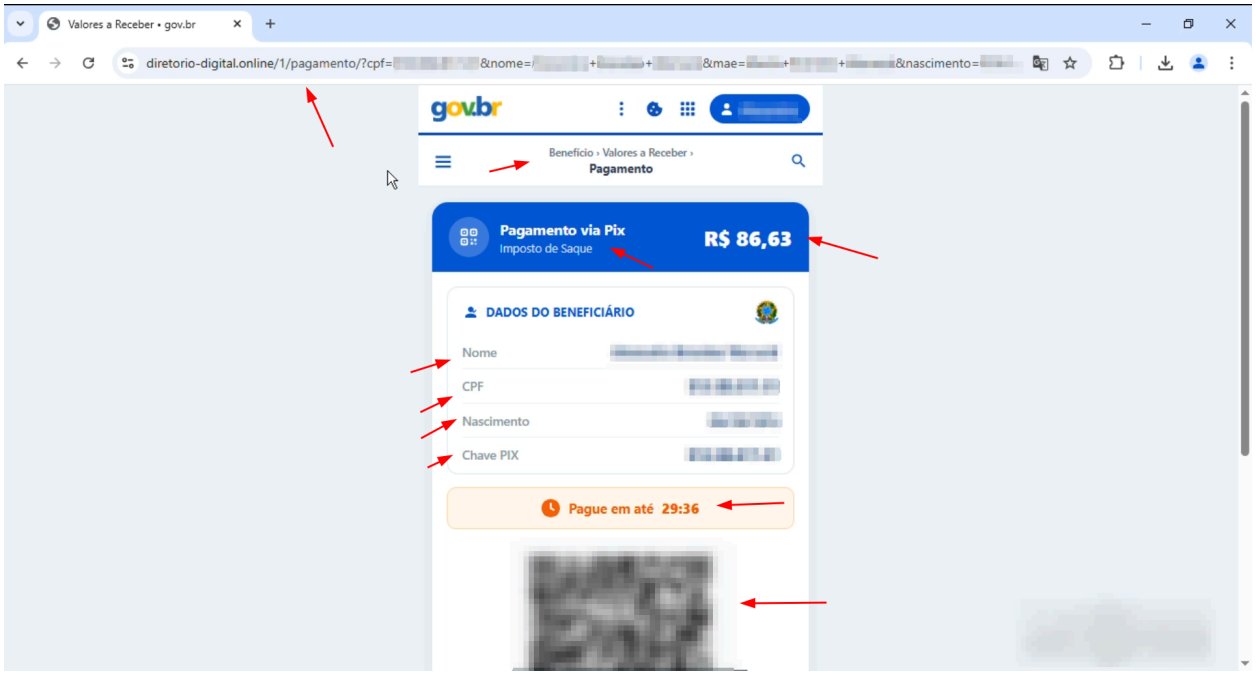



© Lumu Technologies, Inc. All rights reserved.

O sistema gera um comprovante fraudulento oficial do saque, explicando a razão do imposto reembolsável e exibindo o código QR de cobrança Pix com tempo limite de expiração.




© Lumu Technologies, Inc. All rights reserved.

## Vertente Financeira: Nubank

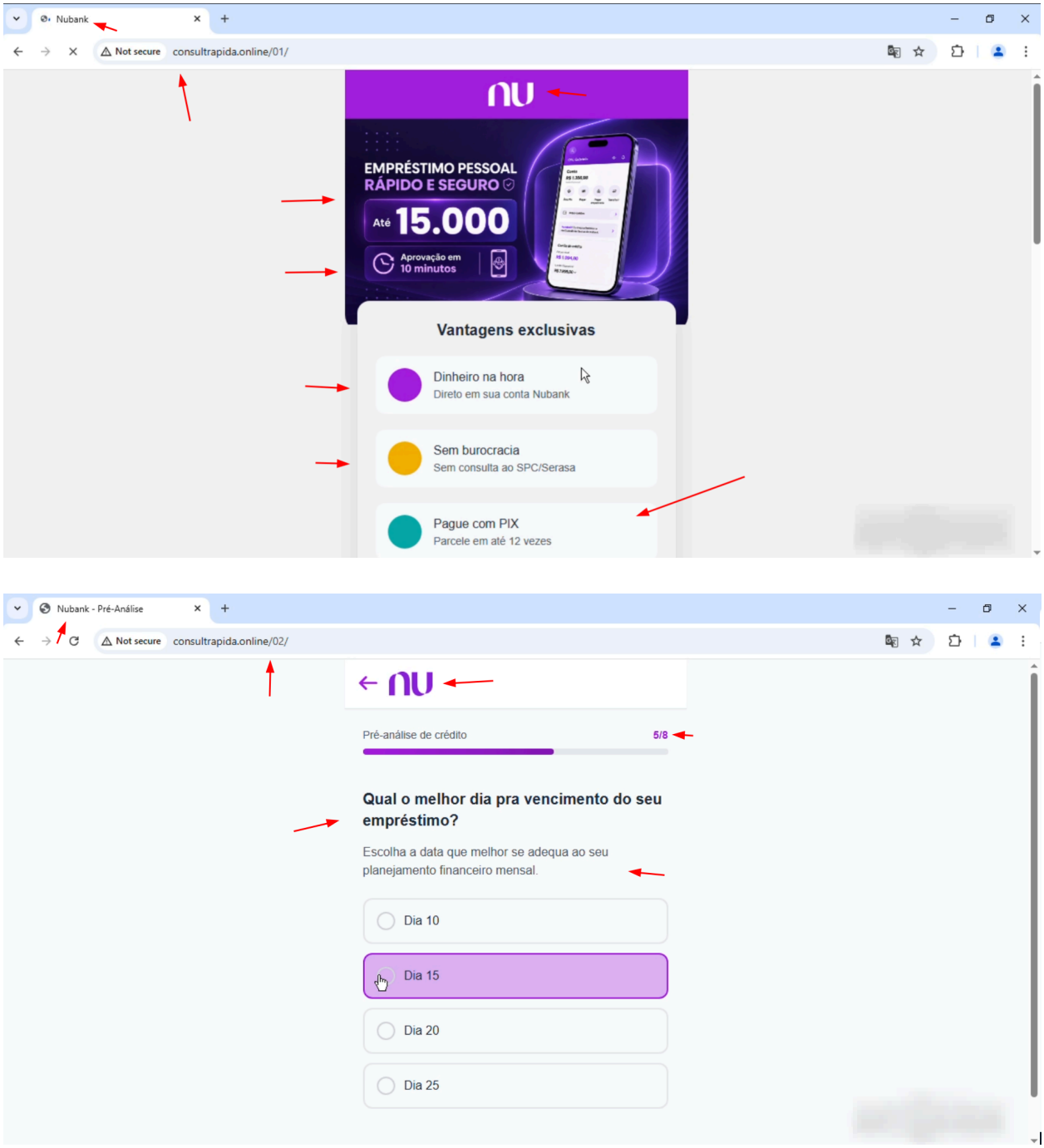
Na vertente comercial, tomou-se como estudo de caso o domínio **consultrapida[.]online**, hospedado no endereço IP **192[.]185[.]211[.]243**. Nesse cenário, a isca explora a marca do **Nubank** para oferecer empréstimos pré-aprovados fraudulentos. Seguindo o padrão observado em toda a campanha, o site solicita inicialmente o CPF da vítima para validar e enriquecer a sessão. Em seguida, exibe um questionário de pré-análise dinâmico para simular a avaliação de crédito e conceder uma aprovação fictícia imediata.

Na fase de monetização, o kit notifica uma taxa administrativa de **R$ 28,63** para liberar o desembolso. No entanto, ao redirecionar para o checkout de pagamento, fica evidente uma inconsistência operacional recorrente nesses cenários: o valor final liquidado via Pix sobe para **R$ 28,93**, uma discrepância tarifária provavelmente originada por falhas nos *templates* do kit ou taxas automáticas da plataforma intermediária utilizada pelos cibercriminosos.

A análise dessa transação revelou um elo crítico de infraestrutura: a cobrança compartilha o mesmo recebedor registrado na vertente governamental, identificado sob a razão social truncada "PLITUNI INTERMEDIACAO DE". Essa coincidência consolida a hipótese de um único ator de ameaça (ou uma operação unificada) gerindo a infraestrutura de monetização para ambas as iscas.

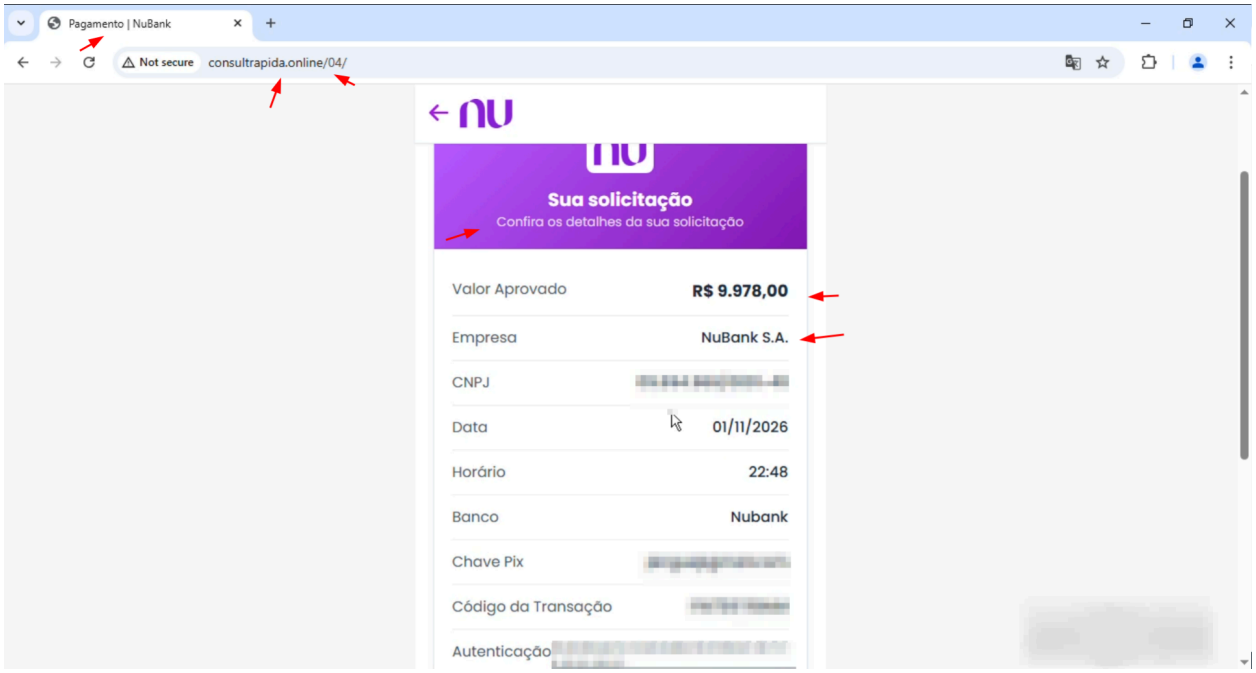
Ademais, em ambas as ramificações da campanha, a cadeia de geração do código Pix aponta para o subdomínio **qrcode.fyhub[.]com[.]br**, a plataforma de pagamentos encarregada de orquestrar a cobrança dinâmica.

© Lumu Technologies, Inc. All rights reserved.

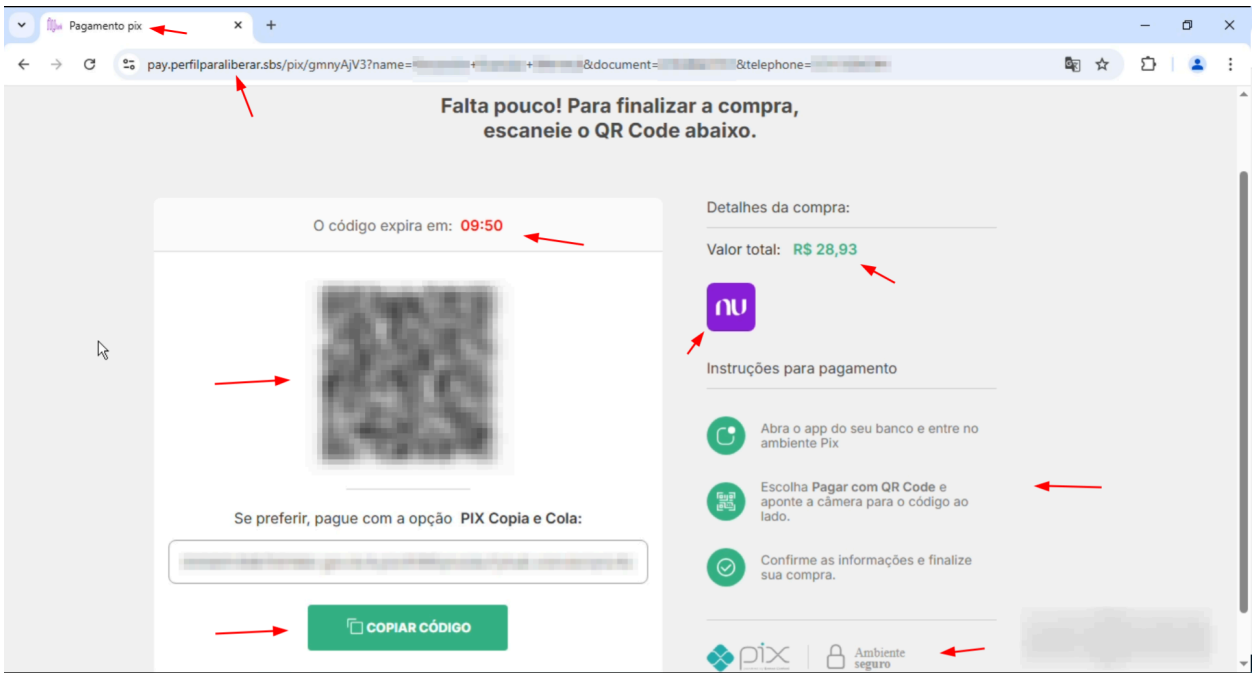



Landing page que se passa pelo Nubank oferecendo empréstimos de até R$ 15.000, aprovação em 10 minutos e sem consulta ao SPC/Serasa. Em seguida, apresenta um questionário falso de pré-análise de crédito que simula a avaliação da vítima.

© Lumu Technologies, Inc. All rights reserved.




A página exibe a confirmação de um empréstimo aprovado de R$ 9.978,00. Após cerca de 4 minutos de espera deliberada para simular o processamento administrativo, o sistema impõe uma janela de 10 minutos para pagar a taxa e redireciona para um checkout que cobra R$ 28,93 via Pix com um código de expiração rápida.




© Lumu Technologies, Inc. All rights reserved.

# Conclusões

- **Infraestrutura unificada e atribuição:** As evidências documentadas nesta investigação confirmam que os três kits analisados convergem em etapas críticas tanto em parte da infraestrutura de hospedagem quanto nos pontos de monetização (compartilhando o mesmo recebedor e os mesmos *endpoints* de QR Code do Pix). Essa sobreposição técnica sustenta a hipótese de um único ator de ameaças (*threat actor*), ou de um grupo criminoso reduzido e coordenado, operando essa arquitetura em um fluxo contínuo e sistemático.
- **Modelo operacional de baixo impacto e alto volume:** O esquema substitui o fraude financeiro tradicional de valores elevados por uma estratégia de monetização granular (*low-and-slow*): a extração em massa de micropagamentos (variando entre R$ 28 e R$ 86). Como essas quantias são mínimas, o ataque reduz a fricção psicológica da vítima para autorizar a transação, mantém-se abaixo dos limites de alerta dos motores antifraude bancários e desestimula a formalização de queixas ou registros de ocorrência perante as autoridades policiais.
- **Superfície de ataque e persistência:** Ao explorar o CPF como chave de identidade digital e se apoiar na instantaneidade irreversível do Pix, esse vetor se consolida como uma das operações de engenharia social mais escaláveis, automatizadas e difíceis de rastrear dentro do ecossistema cibercriminoso brasileiro.
- **Caça proativa e vantagem em inteligência de ameaças:** A expressiva lacuna de visibilidade documentada nesta investigação, em que a Lumu identificou 153 domínios maliciosos frente a apenas 50 catalogados pelos motores convencionais de inteligência web no Q4, reforça a necessidade de abordagens proativas de *threat hunting*. Empresas e clientes que operam no ecossistema brasileiro acessam com exclusividade essa camada de inteligência antecipada por meio dos *feeds* proprietários de telemetria da Lumu. Ao correlacionar infraestrutura de hospedagem e fluxos de monetização em tempo real, essas fontes exclusivas permitem neutralizar o avanço dos ataques e bloquear o tráfego malicioso antes de sua divulgação pública em repositórios abertos.

© Lumu Technologies, Inc. All rights reserved.

# ATT&CK

**6** técnicas em **4** táticas. Matriz Enterprise, ATT&CK v20.0.
**Pasta compartilhada:** mitre_attack_cpf_scam_brazil_en[.]xlsx

# IoCs

Apresentamos os 153 domínios identificados no Q3 e no Q4 de 2026, representando a atividade mais recente desse fenômeno cibercriminoso:

```
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
consultarapidaonline[.]store
```

© Lumu Technologies, Inc. All rights reserved.

```
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
mymixz[.]online
```

© Lumu Technologies, Inc. All rights reserved.

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
ssoriobrsyll[.]site

© Lumu Technologies, Inc. All rights reserved.

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
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
verificadhoje[.]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.