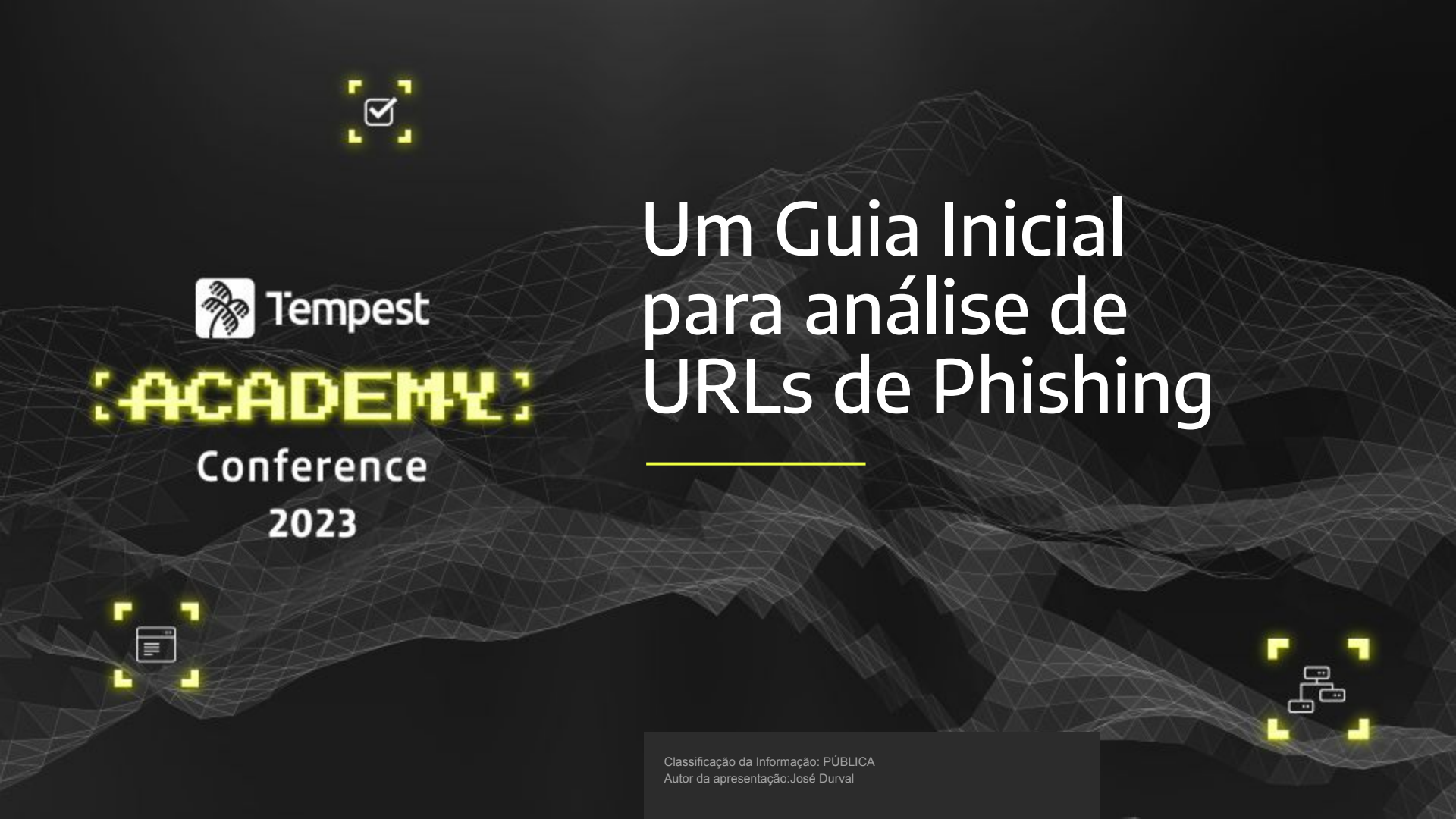


Um Guia Inicial para análise de URLs de Phishing

Classificação da Informação: PÚBLICA
Autor da apresentação:José Durval

Tempest

ACADEMY

Conference

01 Introdução

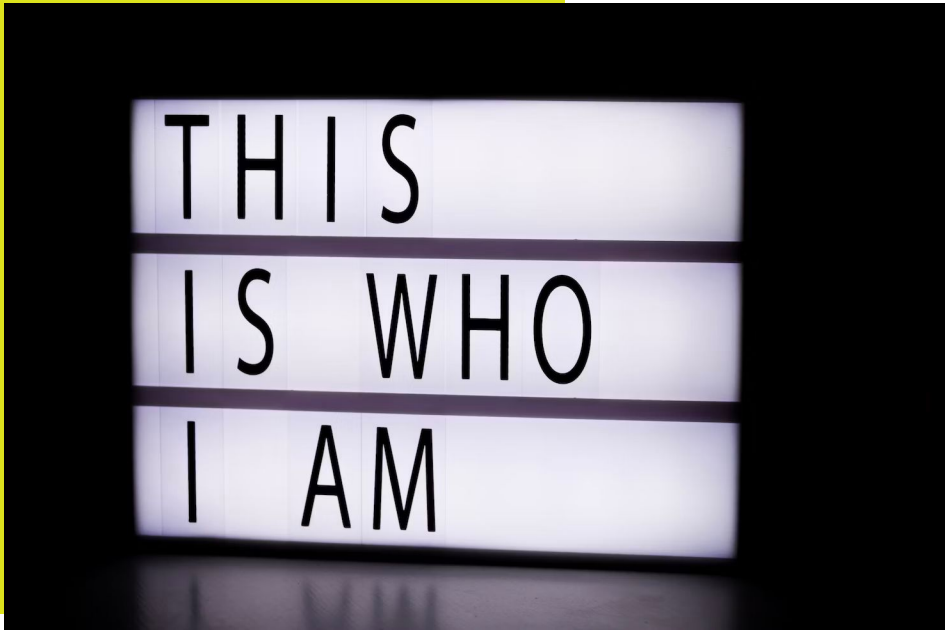
02 Conhecendo o Adversário

03 Ambiente de Análise

04 Análise da Página Falsa

Introdução

Tempest
[ACADEMY]
Conference



Trabalhando na Tempest há quase 10 anos

Praticante e pesquisador de Threat Intelligence

Atuei diretamente no combate a mais de 10 mil campanhas de Phishing

Lidero um time que tem como foco ajudar negócios a tomarem conhecimento sobre as ameaças e se protegerem delas

Objetivos

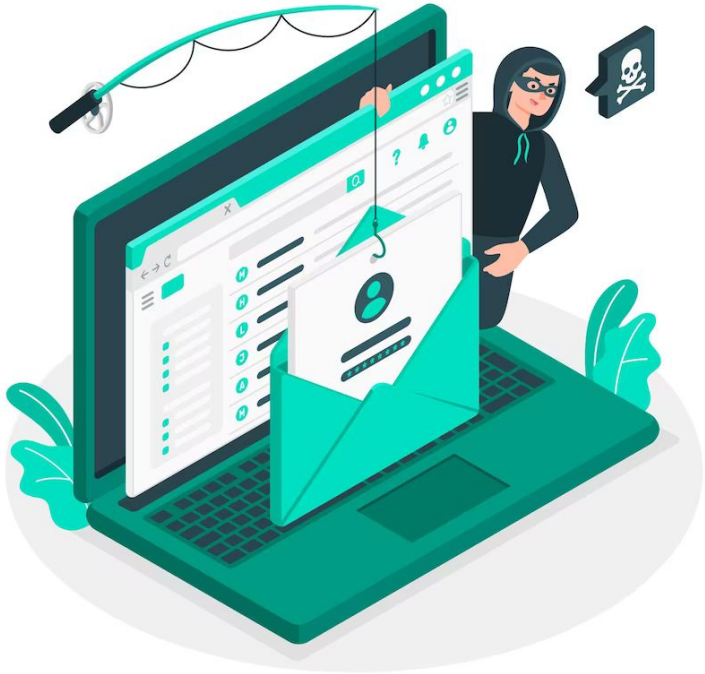
Tempest
ACADEMY
Conference

1. Entender o que é Phishing e a importância de combatê-lo
2. Conhecimentos iniciais para começar a analisar Páginas Maliciosas
3. Dicas para montar seu primeiro laboratório de análise de Phishing
4. Entender técnicas que os atacantes utilizam para dificultar sua análise

Tempest

[ACADEMY]

Conference



Phishing

Phishing

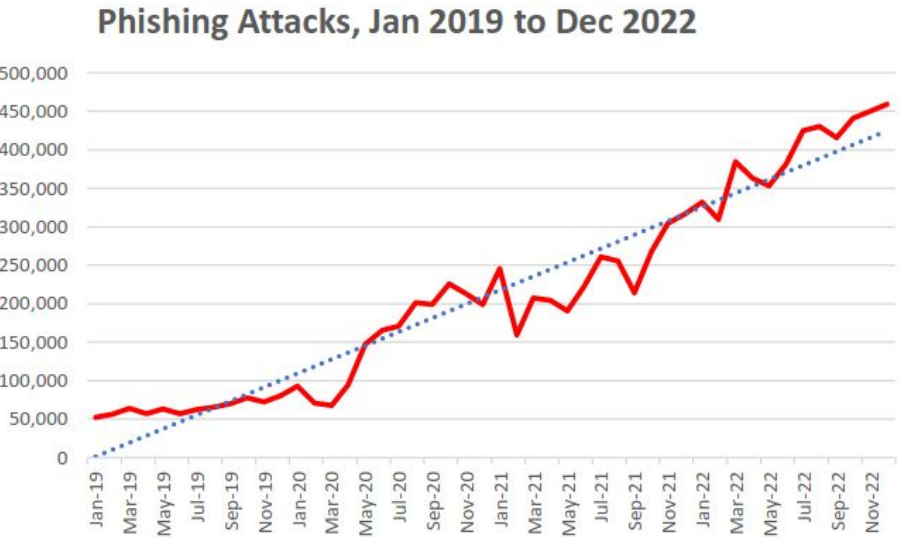
Tempest
[ACADEMY]
Conference

Phishing é um tipo de **ataque** em que criminosos se passam por entidades confiáveis para **enganar** as vítimas e obter **informações pessoais, financeiras ou confidenciais** ou **ganhos financeiros diretos**.

Esse tipo de ataque emprega tanto engenharia social quanto recursos técnicos para enganar suas vítimas.

Phishing

Tempest
[ACADEMY]
Conference



Campanhas de Phishing **cresceram mais de 150% ao ano** nos últimos 4 anos

Phishing

Tempest ACADEMY Conference

Estudo revela que o Brasil é líder m
golpes de phishing

Relatório mostra que um em cada cinco brasileir
menos uma tentativa de ataque em 2020. Já os c
mais de 120% durante a pandemia

Por: Redação, 13/10/2021 às 16h35 - Atualizado em 13/10/2021 às 16h35

2021

Brasil é líder de phishi
na América Latina; sai
se proteger

Fácil de ser executado pelos criminosos, o golpe também é bastante simp

Home > Tecnologia > Brasil é líder de phishing na América Latina; saiba se proteger

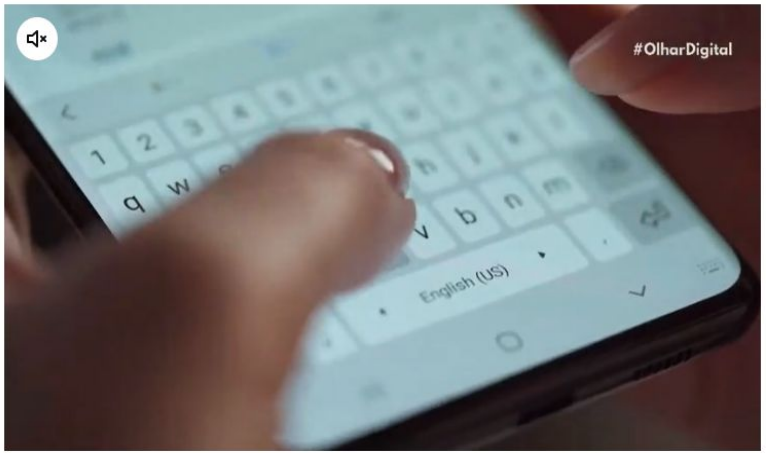
Por Dimitria Coutinho | 18/11/2022 06:00

2022

Brasil é líder em golpes de phishing pelo WhatsApp

Pesquisa da Kaspersky apontou que fraude com link falso foi a mais usada no app em 2022

Tamires Ferreira | 24/03/2023 09h41, atualizada em 24/03/2023 21h02



2023

Tempest

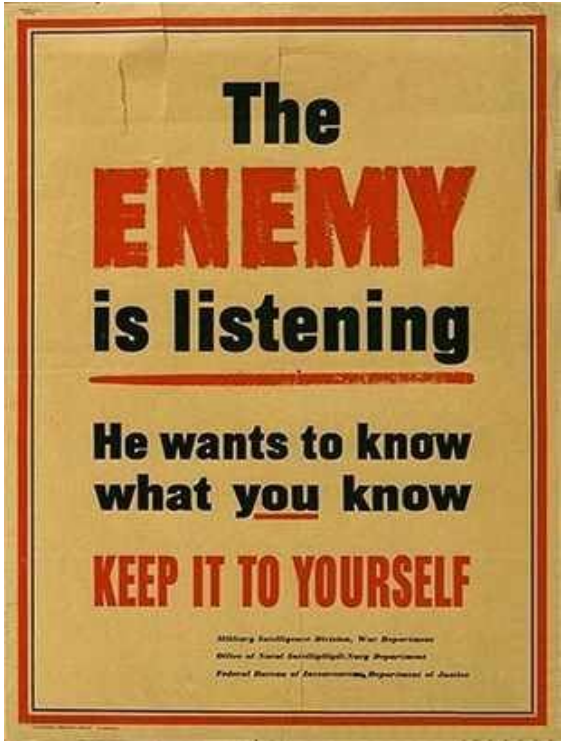
ACADEMY

Conference

Segurança Operacional

Segurança Operacional

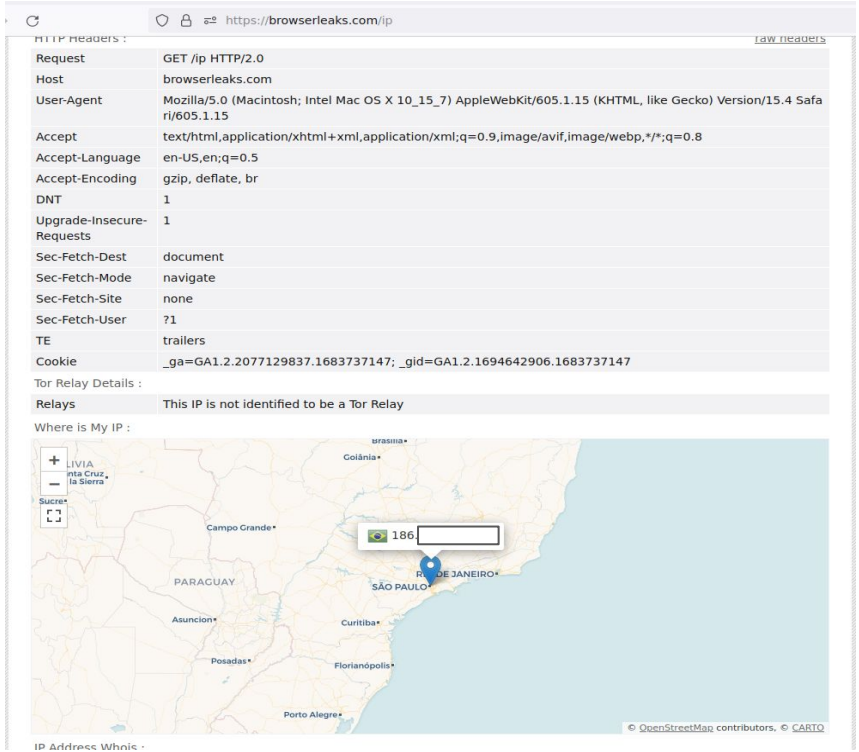
Tempest
[ACADEMY]
Conference



OPSEC envolve vários processos e procedimentos usados para proteger informações que podem ser aproveitadas por adversários

Segurança Operacional

Tempest ACADEMY Conference



Apenas navegando na Internet vocês entrega informações sobre você:

- Qual sistema Operacional
- Qual o seu endereço IP
- Qual a sua geolocalização
- Qual a versão do seu navegador

HTTP Headers : Raw headers

Request	GET /ip HTTP/2.0
Host	browserleaks.com
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.4 Safari/605.1.15
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate, br
DNT	1
Upgrade-Insecure-Requests	1
Sec-Fetch-Dest	document
Sec-Fetch-Mode	navigate
Sec-Fetch-Site	none
Sec-Fetch-User	?1
TE	trailers
Cookie	_ga=GA1.2.2077129837.1683737147; _gid=GA1.2.1694642906.1683737147

Tor Relay Details :

Relays	This IP is not identified to be a Tor Relay

Where is My IP :

Segurança Operacional

Tempest ACADEMY Conference

SWATing: A Prank Where Police Storm Your House

The home of cybersecurity journalist Brian Krebs was flooded by a SWAT team last week pranked into thinking an emergency was happening on his property. He's not alone.

⚠️OBS:ÓBITO DADO NA BASE DO SUS SE CASO O INDIVÍDUO PISAR EM ALGUM HOSPITAL PARA RESOLVER PROBLEMAS MÉDICOS , VAI TA FUDIDO E SERÁ O PIOR ATRASO DA VIDA DELE ❌

➡️01 CPF ÓBITO R$150,00
🟥04 CPF ÓBITO R$350,00

✅ todo o procedimento de operação a Óbito em CPF, iniciamos a gravação da Tela 💻 de execução do serviço do início ao fim, executamos uma nova realização de consulta ao CPF do bico no banco de dados CADSUS pra que assim seja feita a verificação e a checagem da veracidade, no êxito na realização do Óbito ao CPF desejado. ✅

[redacted] ▶ [redacted]

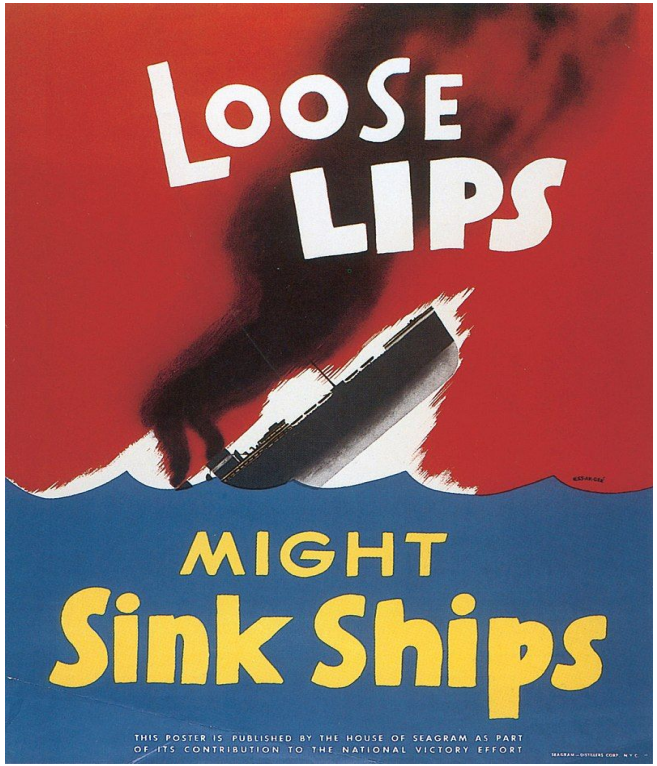
8 de janeiro · 🌐

ABRO LARA EM UM BANCO CPF ESPECÍFICO, PIX ATIVO E DEPENDENDO DO SCORE DEPOIS DE UM TEMPO SOLTA UM EMPRÉSTIMO PESSOAL VEM 🧧

1 1 comentário

Segurança Operacional

Tempest
[ACADEMY]
Conference



Medidas para manter o OPSEC:

- Personas
- Ambiente virtualizado
- Saídas anonimizadas

Conhecendo o Adversário

Tempest

[ACADEMY]

Conference

Conhecimento Técnico

Motivação

Entendimento do Adversário

Tempest
[ACADEMY]
Conference

Exemplos de técnicas de bloqueio de conteúdo

Tempest
ACADEMY
Conference

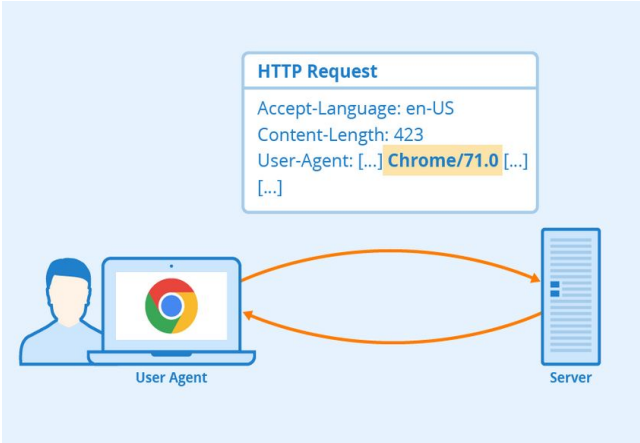
Bloqueio por Origem

```
<limit GET POST PUT HEAD>
order deny,allow
allow from 179.
allow from 186.
allow from 187.
allow from 189.
allow from 191.
allow from 192.
allow from 198.
allow from 200.
allow from 201.
deny from 150.70.173.
deny from 213.190.193.
deny from 81.161.59.
deny from 70.39.157.
deny from all
</limit>
```

```
$ListaBanidos = array("scotiabank","letti.","unisys","
    antivirus1.unisys","antivirus","abuse@","spam@", ".sysms.net
    ", "easysol.net", "diebold", "cisco.com", "antivirus2.unisys
    ","hawking.unisys","ragingwire.net", "isitphishing.org", "
    barracuda","netcraft", "ebay.", "panda.","microsoft.","fbi."
    , "google.", "resuelveserver", "bankofamerica", "mozilla.",
    "viabcp.", "veritas.","nod32.","antipishing.","kapersky.", "
    norton.", "symantec.","rsasecurity.", "bancopopular.", "
    paypal.", "unicaja.", "movistar.", "banesto", "cajamadrid",
    "bancopastor", "rsa.", "symantecstore.", "gfihispana.", "
    fraudwatchinternational.", "verisign.", "markmonitor.", "
    anti-phishing.", "pandasoftware.", "delitosinformaticos.", "
    zonealarm", "alerta-antivirus", "vsantivirus", "
    nortonsecurityscan", "hauri-la", "cleandir", "trendmicro", "
    mcafee", "nod32-es", "pandaantivirus", "free-av", "grisoft"
    , "bitdefender-", "sophos", "activescan", "avast", "
    bitdefender", "trendmicro-europe", "clamav", "clamwin", "
```

Tempest
ACADEMY
Conference

Bloqueio por Dispositivo

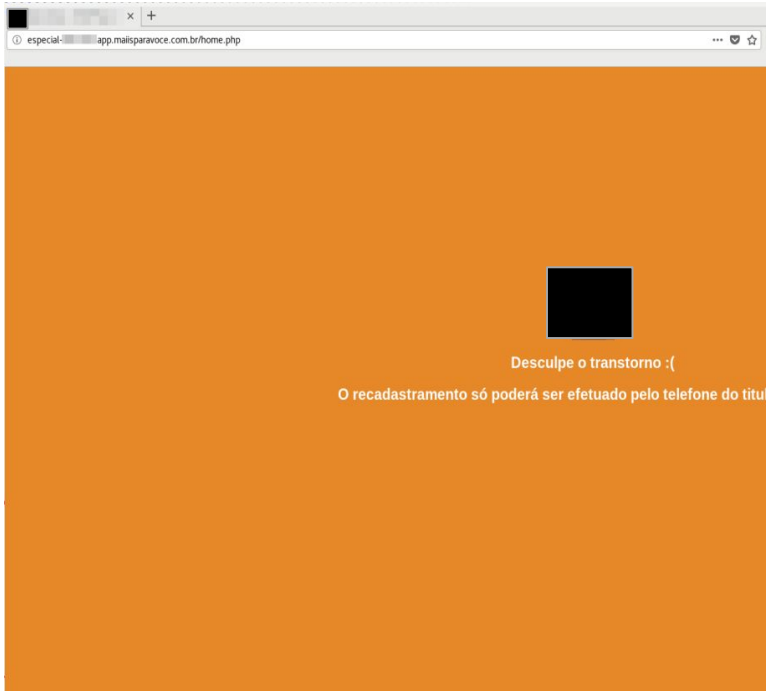



```
<script>
var suamae = navigator.userAgent.toLowerCase();
var uMobile
uMobile = '';
uMobile += 'iphone;ipod;windows phone;android;iemobile 8';
v_uMobile = uMobile.split(';');
var boolMovel = false;
for (i=0;i<=v_uMobile.length;i++){
  if (suamae.indexOf(v_uMobile[i]) != -1){
    boolMovel = true;
  }
}
if (boolMovel != true){
  location.href='http://xxxx.eu';
}
</script>
```

Tempest
ACADEMY
Conference

Bloqueio por Tela

Tela tamanho desktop



Tela tamanho mobile

Tempest

ACADEMY

Conference

Ambiente de Análise

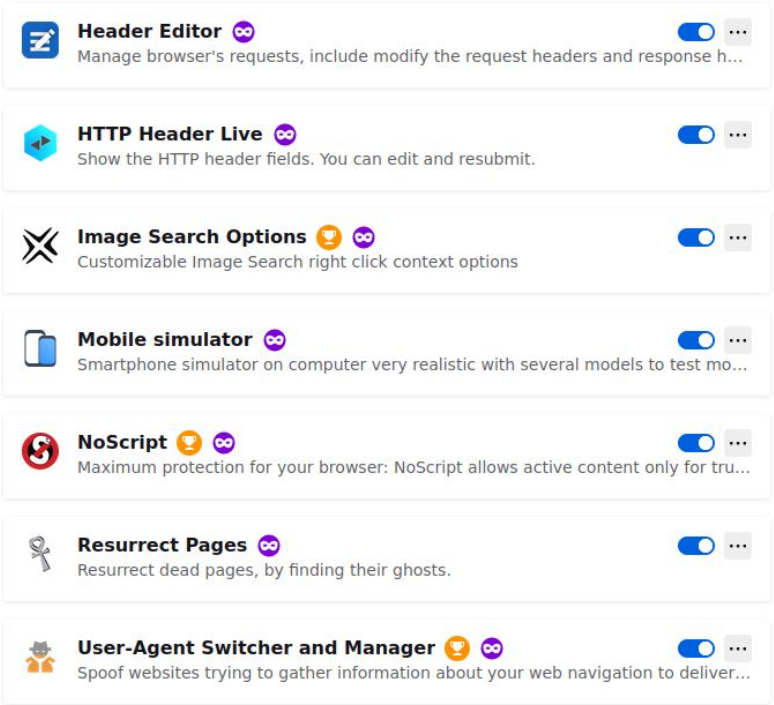
Virtualização

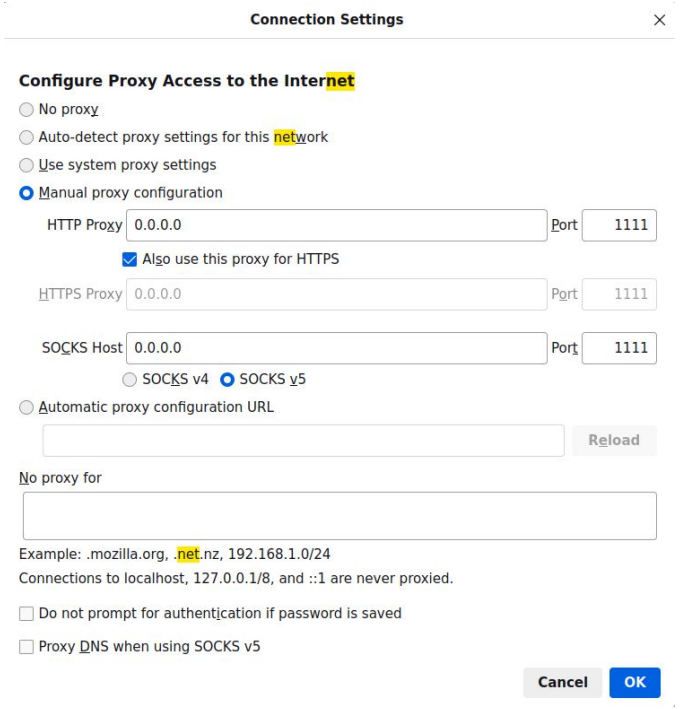
Tempest
ACADEMY
Conference

Navegador

Navegador

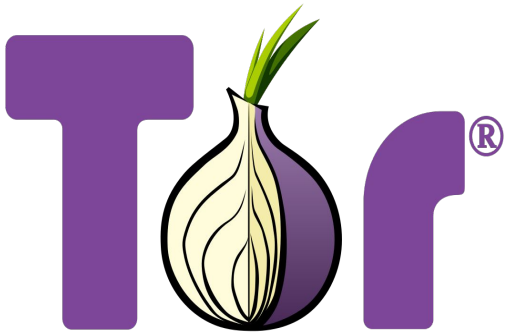
Tempest
[ACADEMY]
Conference





Saída Anonimizada

Tempest
[ACADEMY]
Conference



TorProject.org

Setup para começar

Tempest
[ACADEMY]
Conference

+

+

Tempest

:ACADEMY:

Conference

Análise da Página Falsa

Tempest

ACADEMY

Conference

URL

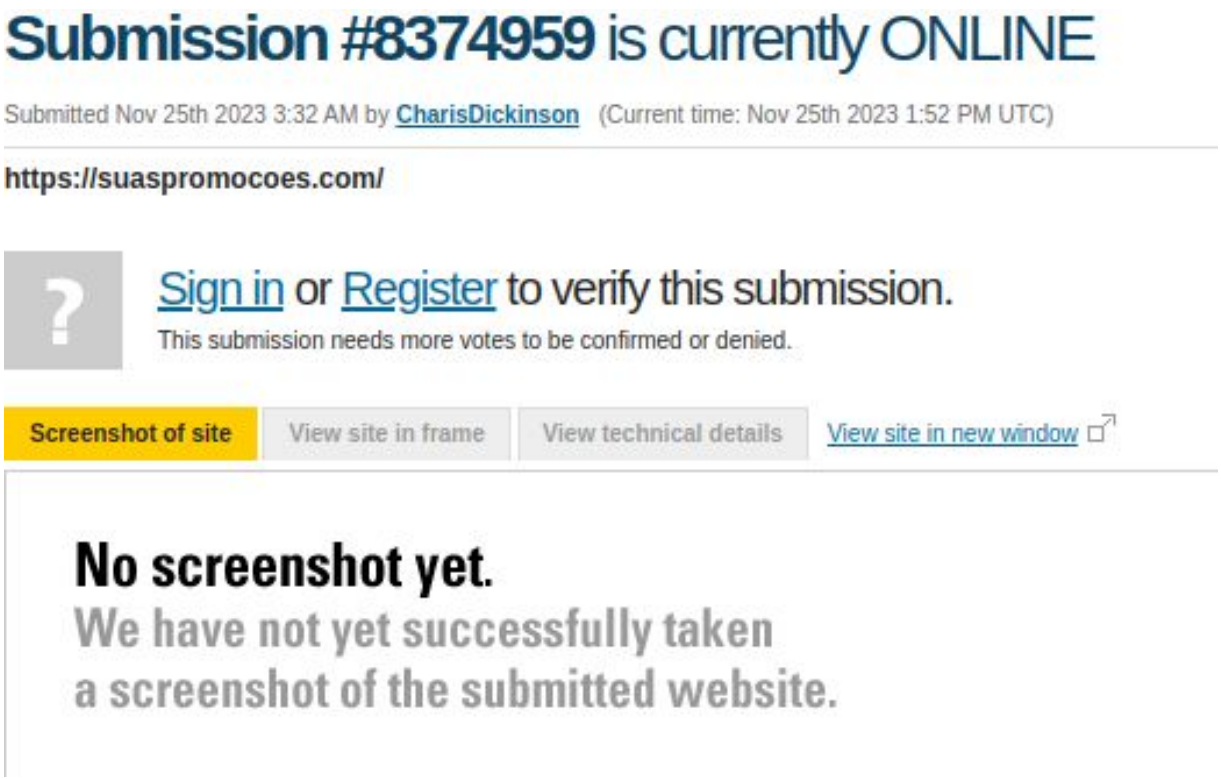
Elementos da URL

Tempest
ACADEMY
Conference

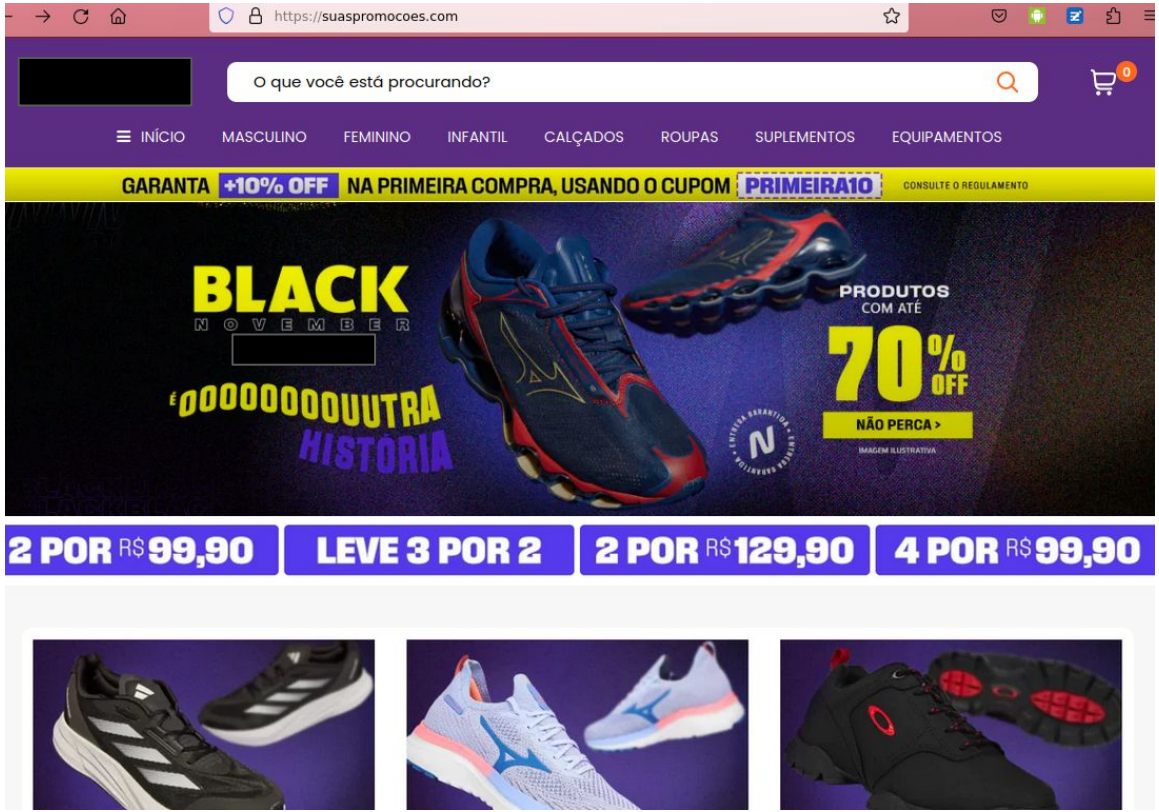
- **Site Comprometido/ Domínio Malicioso**
- **Informações do Host/Registrar**
- **Parâmetros da URL**

Elementos da URL

Tempest
ACADEMY
Conference



Elementos da URL



Elementos da URL

Tempest
ACADEMY
Conference

suaspromocoes.com

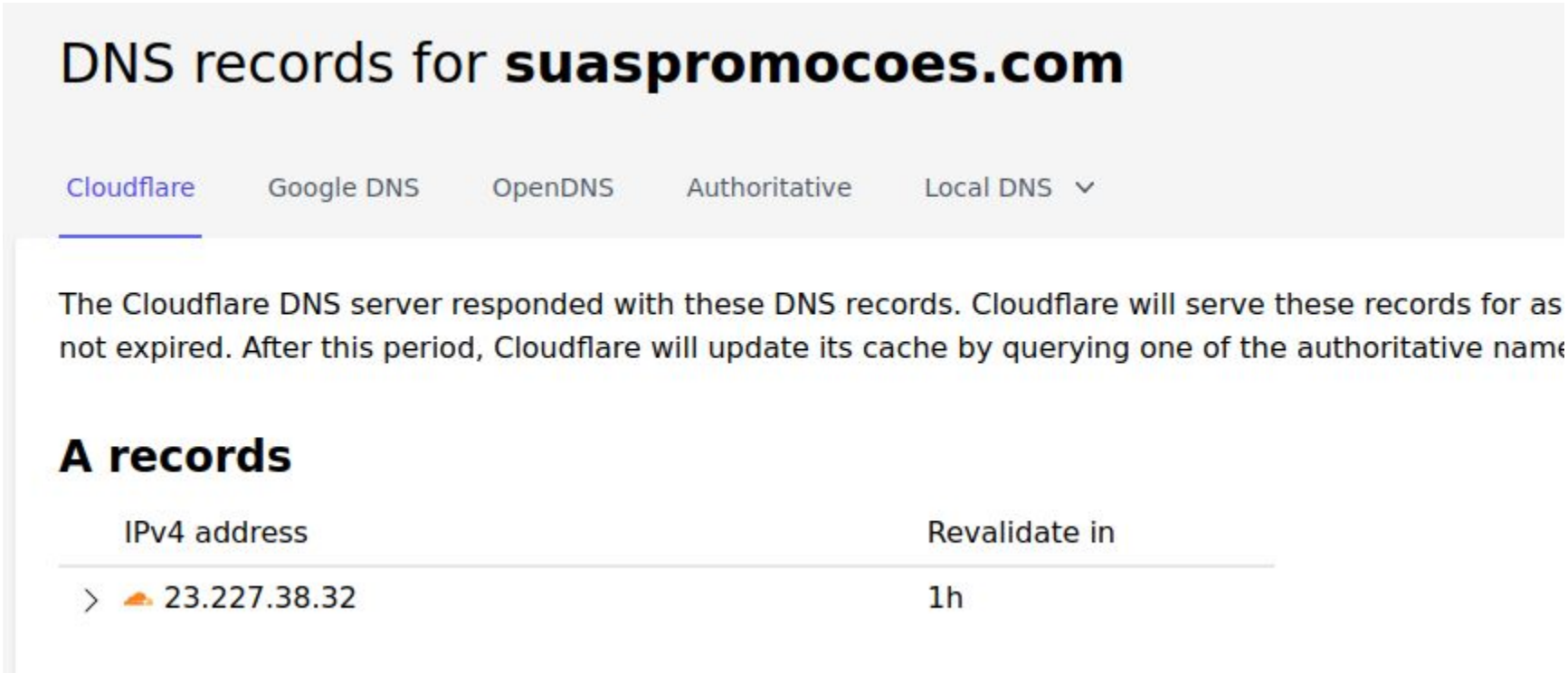
Updated 11 hours ago

Domain Information

Domain:	suaspromocoes.com
Registrar:	GoDaddy.com, LLC
Registered On:	2023-11-24
Expires On:	2024-11-24
Updated On:	2023-11-24
Status:	clientDeleteProhibited clientRenewProhibited clientTransferProhibited clientUpdateProhibited
Name Servers:	ns07.domaincontrol.com ns08.domaincontrol.com

Elementos da URL

Tempest
ACADEMY
Conference



Elementos da URL

Tempest
[ACADEMY]
Conference

- **Site Comprometido/ Domínio Malicioso?**
  - Domínio Malicioso
- **Informações do Host/Registrar**
  - Godaddy
  - CloudFlare
- **Parâmetros da URL**
  - N/A

Tempest
ACADEMY
Conference

Navegar na Página

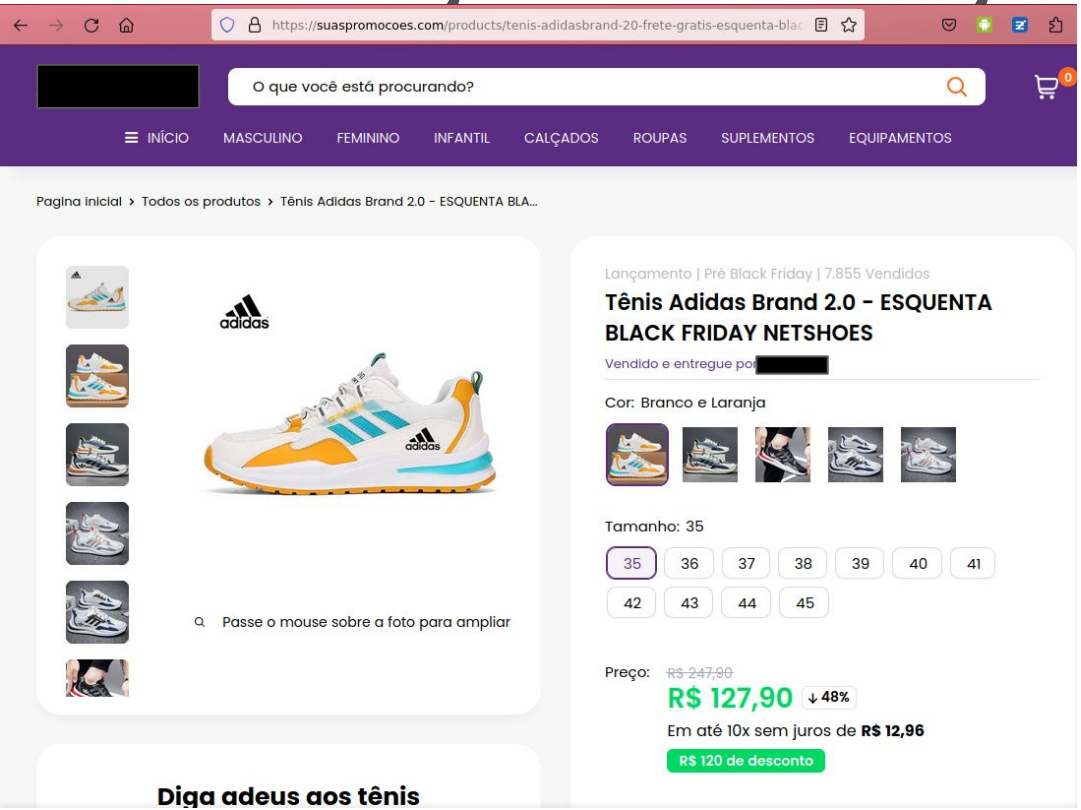
Navegar na Página

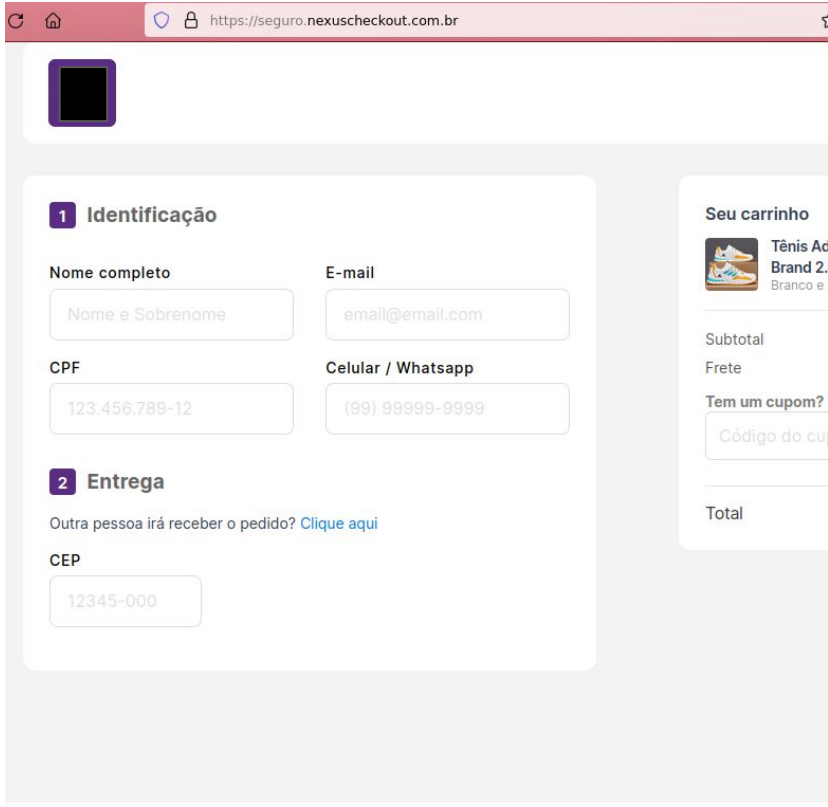
Tempest
[ACADEMY]
Conference

- **Qual é o fluxo do Phishing?**
- **Quais informações são solicitadas?**
- **Existe algum tipo de bloqueio?**
- **Qual é o público-alvo da campanha?**

Navegar na Página

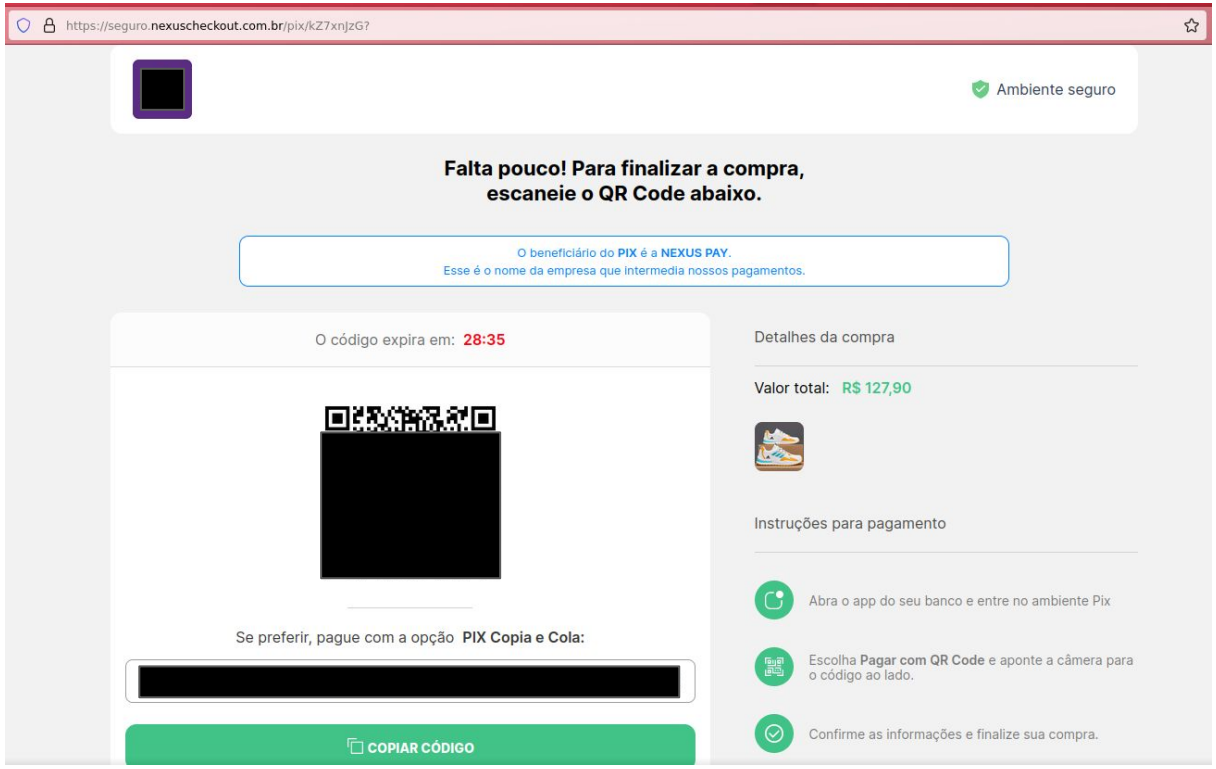
Tempest
[ACADEMY]
Conference





Navegar na Página

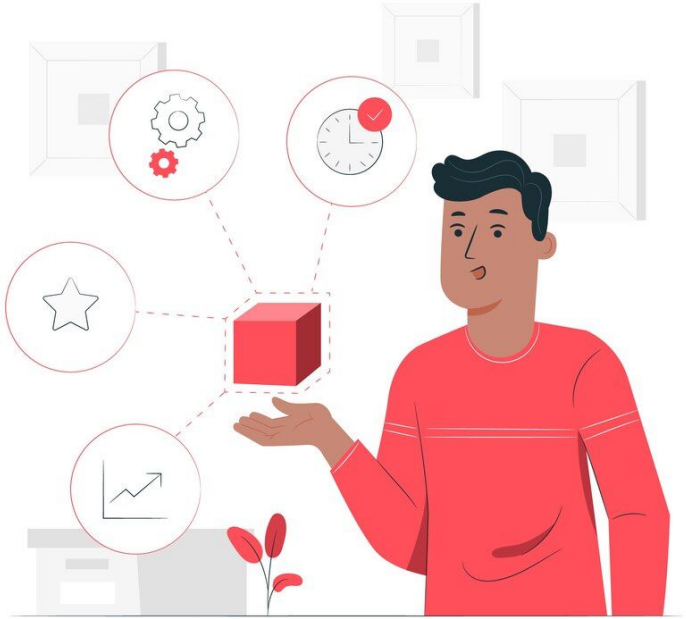
Tempest
[ACADEMY]
Conference



Tempest

[ACADEMY]

Conference



Resumindo

Resumindo

Tempest
ACADEMY
Conference

- Domínio Malicioso recém registrado na Godaddy e site na Cloudflare
- Página sem Bloqueio, focada no público em geral e utilizando processador legítimo de pagamentos.

Considerações Finais

Objetivos

Tempest
[ACADEMY]
Conference

1. Entender o que é Phishing e a importância de combatê-lo ✓
2. Conhecimentos iniciais para começar a analisar Páginas Maliciosas ✓
3. Dicas para montar seu primeiro laboratório de análise de Phishing ✓
4. Entender técnicas que os atacantes utilizam para dificultar sua análise ✓

Próximos Passos

Tempest
ACADEMY
Conference

- Analisar código-fonte da Página
- Analisar requisições executadas pela página Maliciosa

Links Úteis

Tempest
[ACADEMY]
Conference