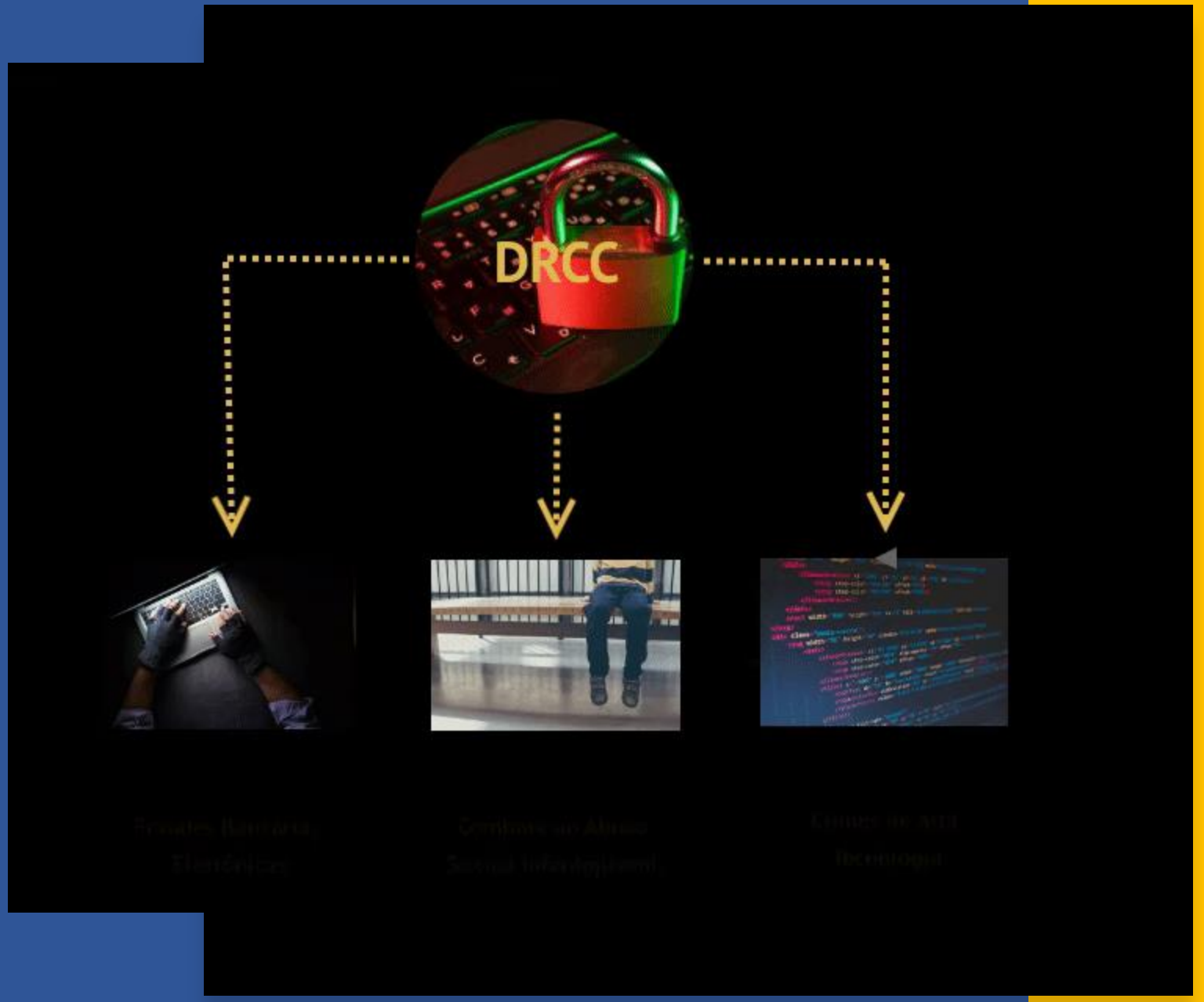
Vestígios eletrônicos, investigação e a perícia nos crimes cibernéticos

São Paulo, 06 de novembro de 2023.

Eixos Distintos



DIRETRIZES CONSTITUCIONAIS

Constituição Federal ⚖ Art. 227.

É dever do Estado assegurar com **absoluta prioridade** seus direitos, além de colocá-los a salvo de toda forma de exploração

§ 4º A lei punirá severamente o abuso, a violência e a exploração sexual da criança e do adolescente.

IDENTIFICAÇÃO E RESGATE

Repressão à produção, posse e distribuição de material de abuso sexual infantojuvenil

Foco principal na identificação e resgate de vítimas

VESTÍGIOS EM CRIMES RELACIONADOS AO ABUSO SEXUAL INFANTOJUVENIL

Perfil do criminosos

Sextortion

Deepfake

VESTÍGIOS EM CRIMES RELACIONADOS AO ABUSO SEXUAL INFANTOJUVENIL

Moderação IA

Remoção de conteúdo

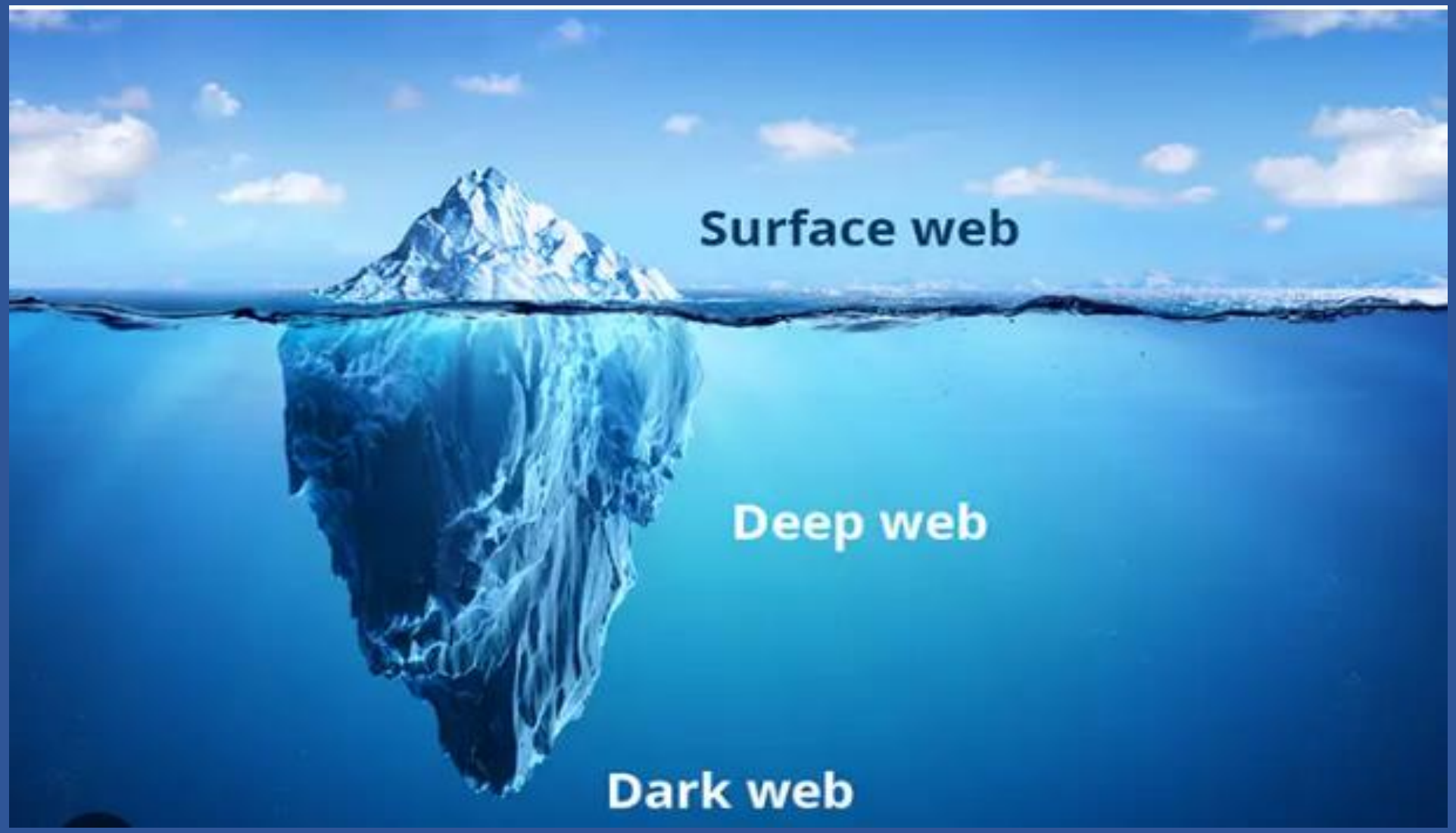
Violação de termos de uso

VESTÍGIOS EM CRIMES RELACIONADOS AO ABUSO SEXUAL INFANTOJUVENIL

PRIVACIDADE

VESTÍGIOS EM CRIMES RELACIONADOS AO ABUSO SEXUAL INFANTOJUVENIL

PRIVACIDADE ou **CONIVÊNCIA?**


Surface web
Deep web
Dark web

VESTÍGIOS EM FRAUDES BANCÁRIAS ELETRÔNICAS

O GLOBO 80 anos

IRINEU MARINHO (1876-1925) RIO DE JANEIRO, TERÇA-FEIRA, 9 DE AGOSTO DE 2005 • ANO LXXXI • Nº 26.300 • www.oglobo.com.br ROBERTO MARINHO (1904-2003)

Tuno Vieira/Diário do Nordeste

Jarbas Oliveira

Bando usa túnel para roubar R$ 156 milhões

PF diz que assalto ao Banco Central em Fortaleza é o maior da História do país

• Bandidos entraram na caixa-forte do Banco Central em Fortaleza por um túnel de 80 metros de extensão e roubaram R$ 156 milhões, no maior assalto do país, segundo a Polícia Federal. Os sensores de movimento e as câmeras de vigilância do cofre não funcionaram. Quatro contêineres com cédulas de R$ 50 foram esvaziados e um quinto apenas parcialmente. Os ladrões desprezaram notas novas e seriadas para evitar rastreamento. O túnel, cavado por três meses, foi revestido de madeira e lona e tinha luz e ar-condicionado. O buraco começa numa casa alugada a um quarteirão do BC, onde foi aberta a empresa de fachada Grama Sintética, para facilitar a retirada do entulho. Página 12

• Policiais e jornalistas observam a entrada do túnel usado pelos bandidos, numa casa a um quarteirão de distância do prédio-sede do Banco Central em Fortaleza.

BANCO CENTRAL DO BRASIL

R$ 156 MILHÕES

Quadrilha queria R$ 90 milhões em banco de Araçatuba, mas dinheiro foi rasgado

Quadrilha deixou cerca de 40 explosivos espalhados em Araçatuba (Foto: Divulgação/Gate PM SP)

R$ 4,5 MILHÕES

R$ 15 MILHÕES em jóias

exame.

Inteligência Artificial

Home › Inteligência Artificial

Com R$ 2,5 bi em prejuízos por fraudes, BC estuda responsabilizar bancos por golpes; IA pode ajudar?

veja VEJA MERCADO RADAR RADAR ECONÔMICO POLÍTICA SAÚDE MUNDO CULTURA ESPORTE AGENDA VERDE

Política

Fraudes no Pix passam de R$ 300 milhões por mês e bancos ficam sob pressão

Golpes passam da média de R$ 10 milhões por dia, são pequenos em relação ao volume de negócios com o PIx, mas ameaçam a confiança no sistema de pagamentos

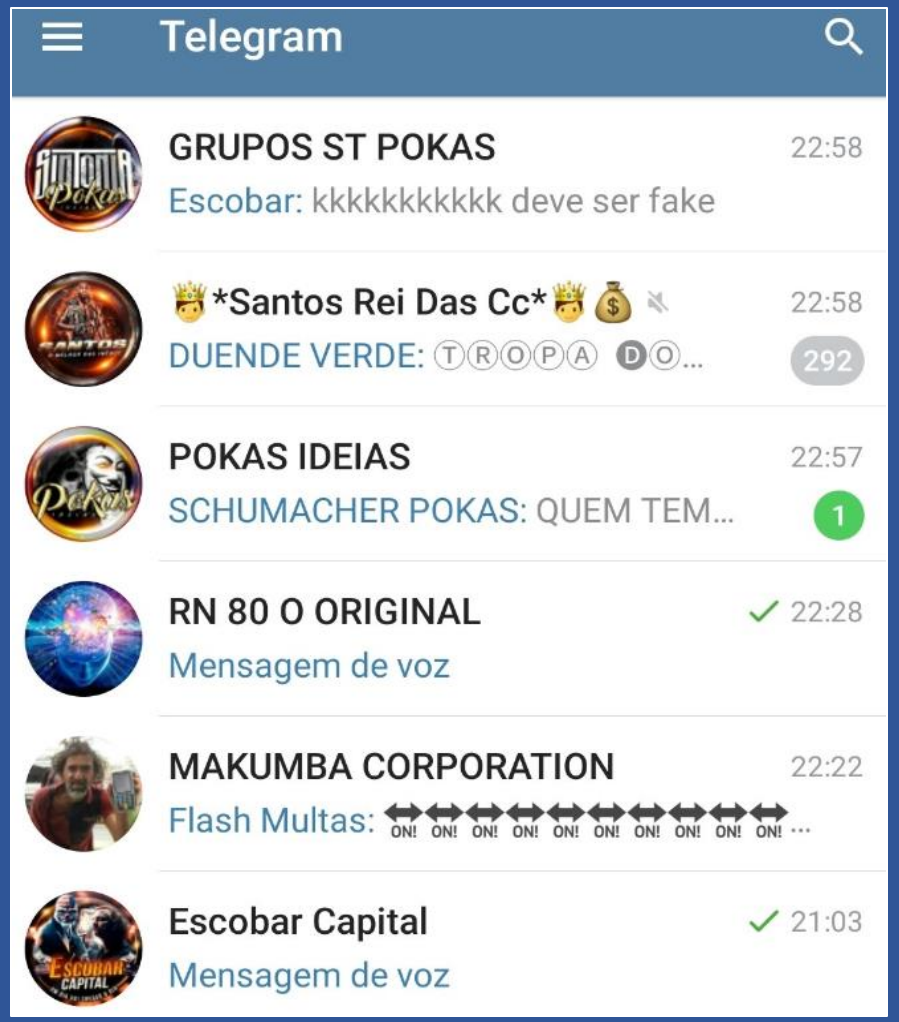
CNN BRASIL

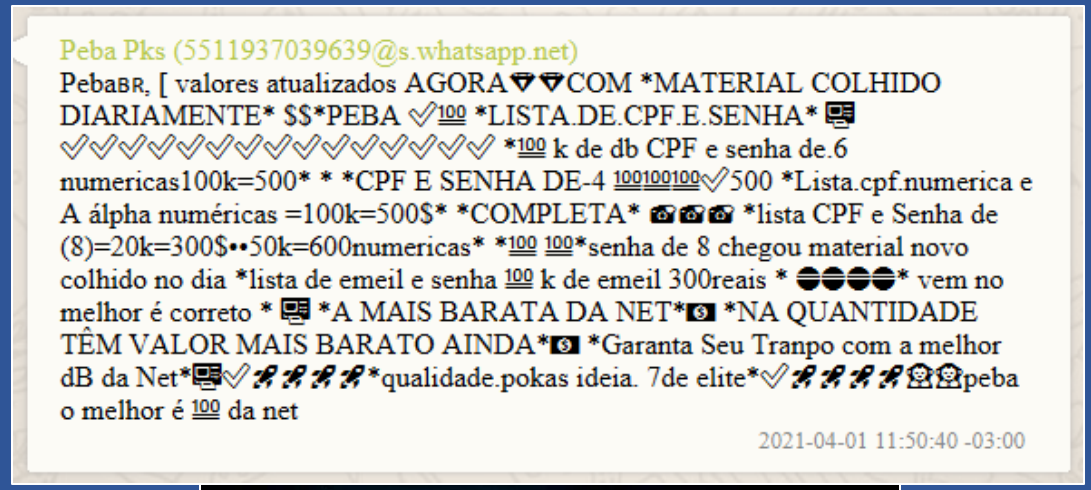
Mais de 1,7 milhão de golpes com Pix foram aplicados em 2022, mostra levantamento

Estudo realizado por fintech também mostra golpes mais recorrentes, confira

FRAUDES BANCÁRIAS ELETRÔNICAS

MODO DE OPERAÇÃO





MODO DE OPERAÇÃO

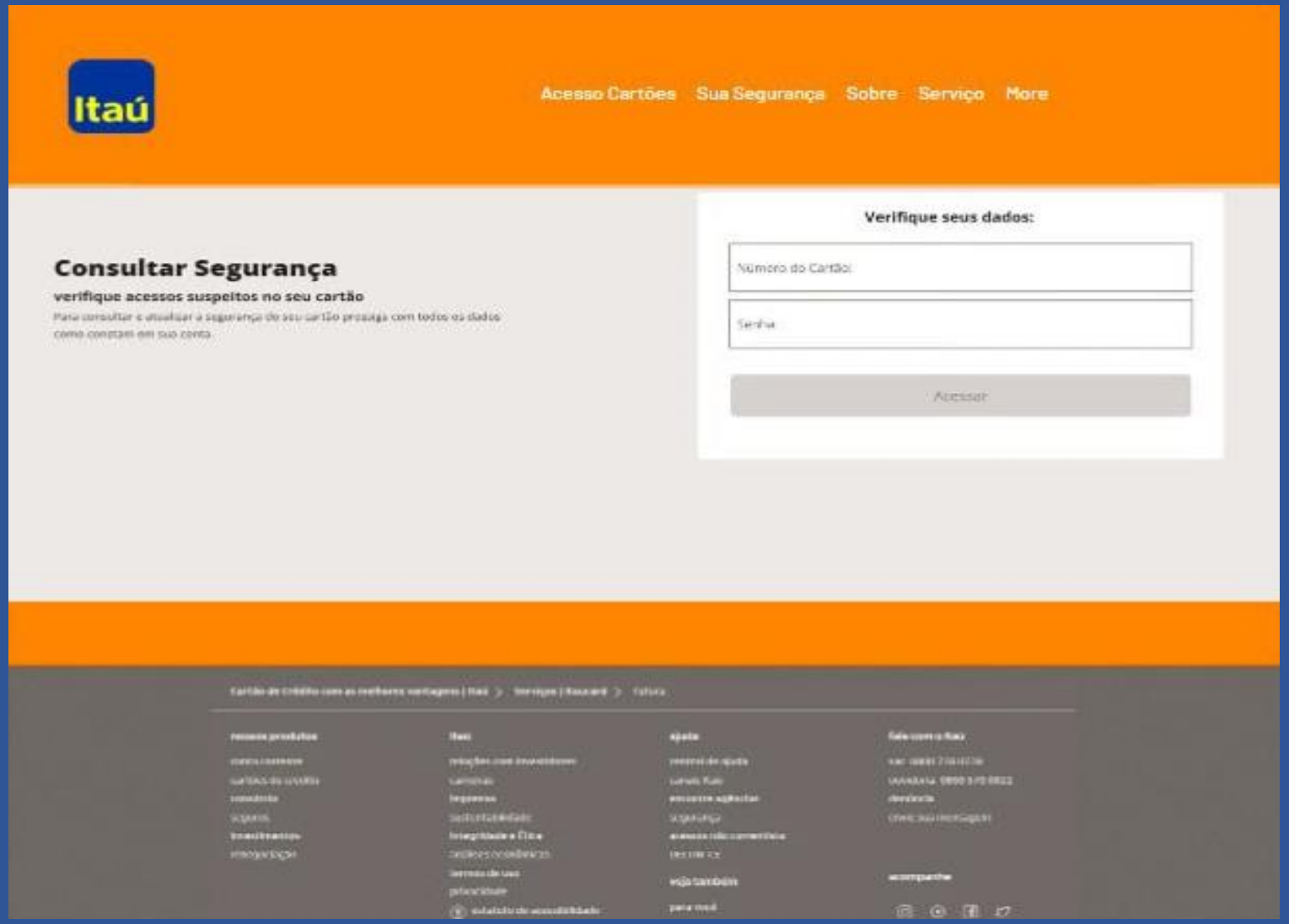
VENDA DE LOGIN E SENHA

VENDA DADOS

DADOS DE CARTÕES

PÁGINAS FALSAS

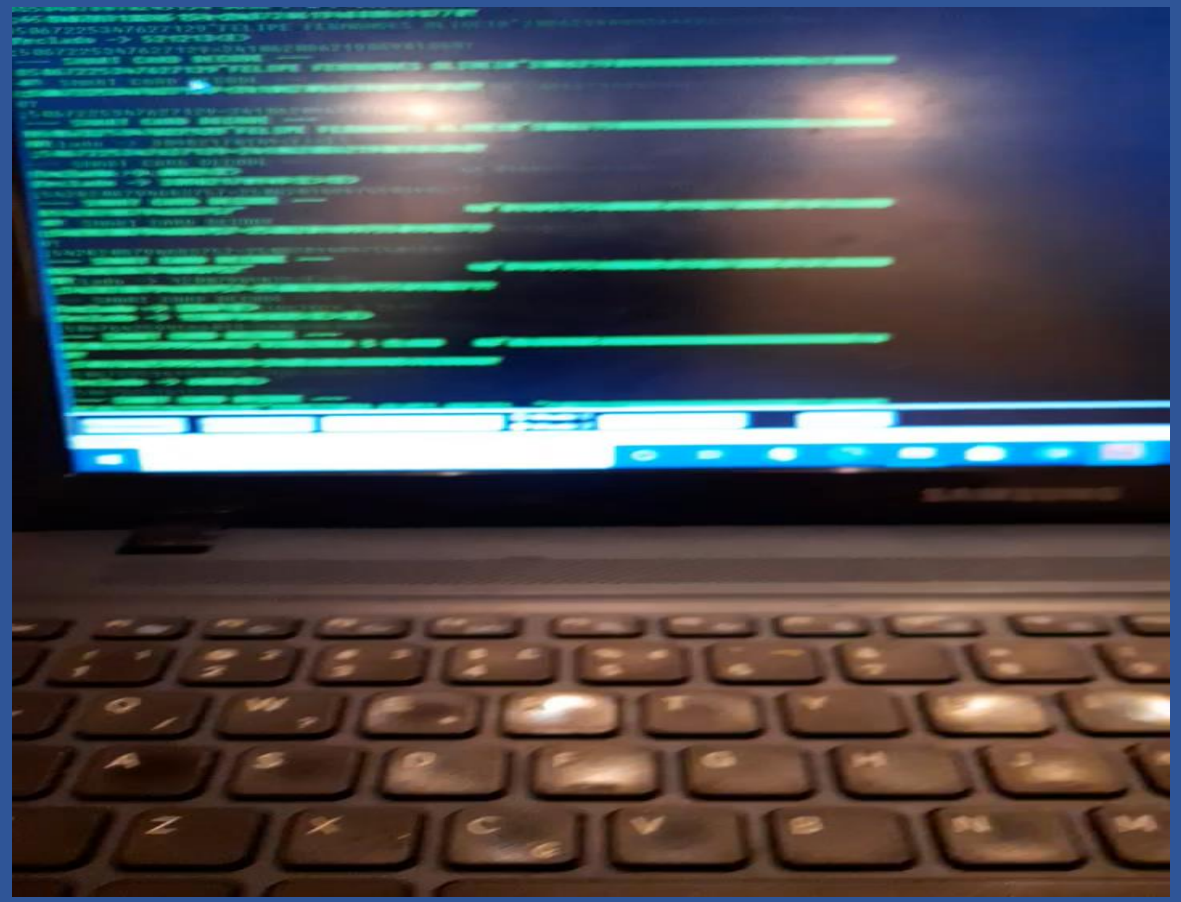
ENGENHARIA SOCIAL



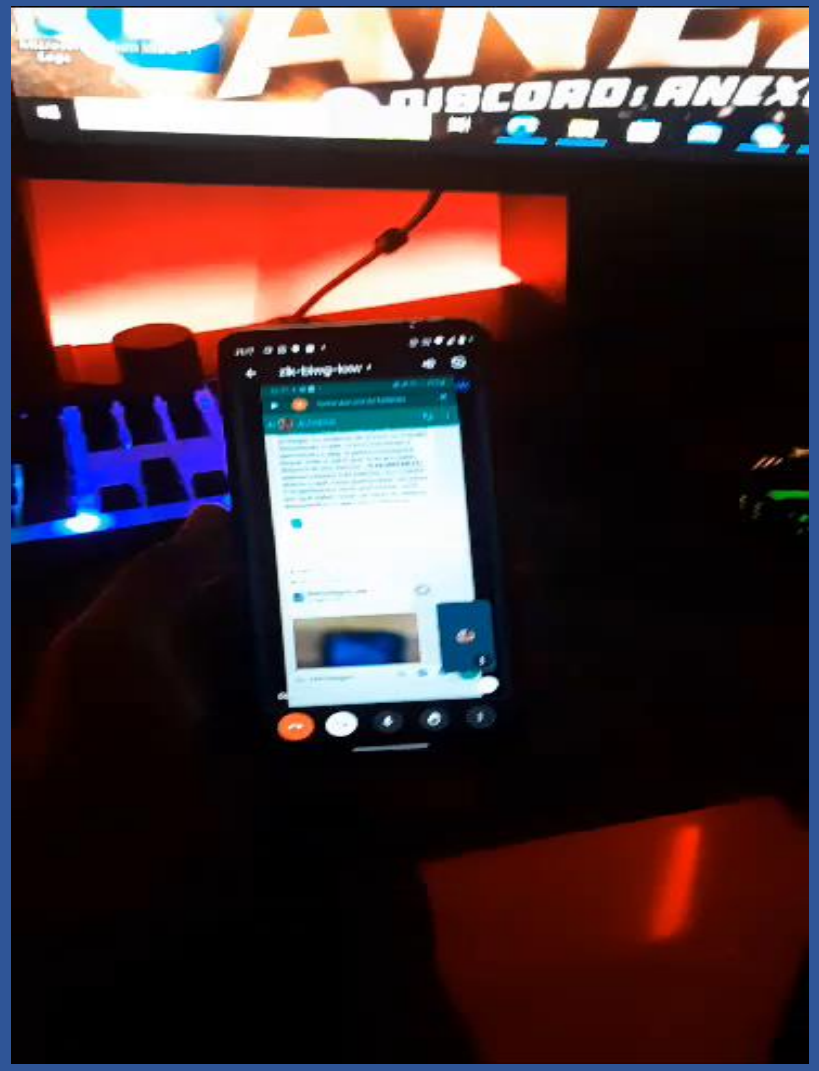
OBTENÇÃO E COMÉRCIO DE DADOS

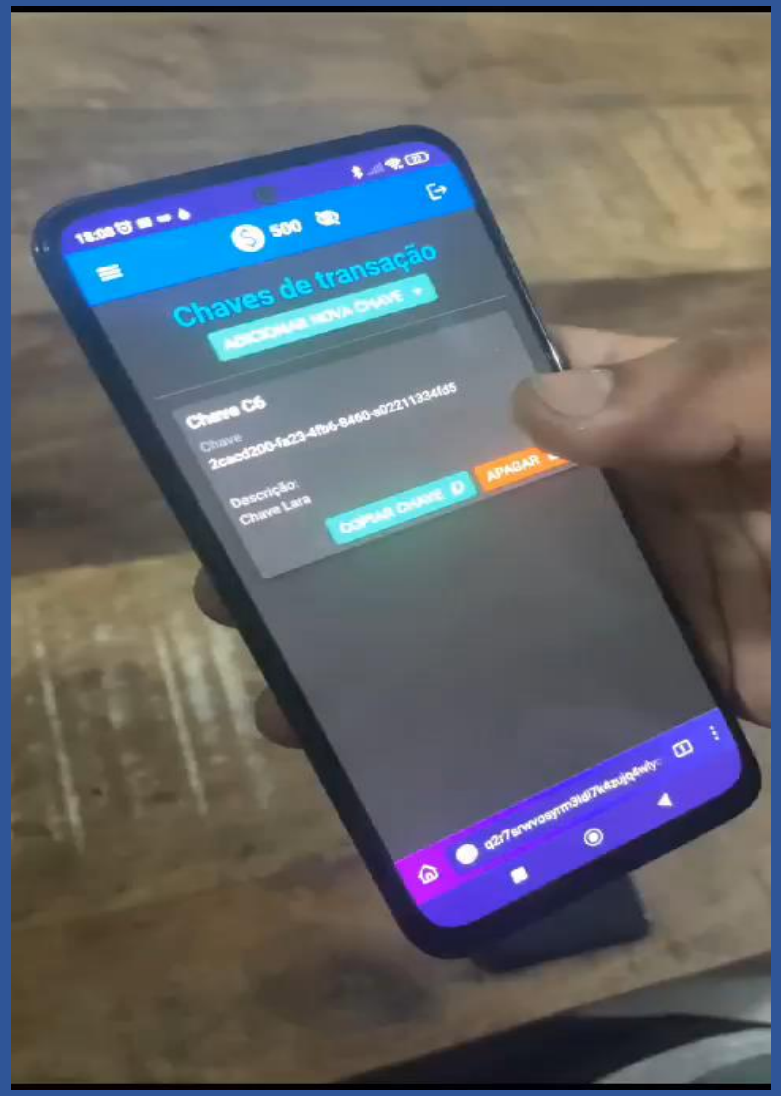
Dispositivo de clonagem instalados em maquinetas

Deixa eu te falar, amanhã a máquina vai entrar aí tá? Nesse estabelecimento aí, no ***Giraffa's, no Shoppinzinho aqui a beira mar****, beleza meu amor? Shoppinzinho aqui de frente pro mar. Amanhã, quando eu for lá amanhã, eu te mando as fotos direitinho e os vídeos de lá, mas lá é bem movimentado.*



MODO DE OPERAÇÃO - FRAUDE PIX





FRAUDES BANCÁRIAS ELETRÔNICAS

PECULIARIDADES

- ✓CRIMES MASSIVOS
- ✓MULTITERRITORIALIDADE
- ✓RESPOSTA TRADICIONAL INADEQUADA

MÉTODO

SISTEMA TENTÁCULO

MÉTODO

SISTEMA TENTÁCULOS

MÉTODO TRADICIONAL

INVESTIGAÇÃO EM SENTIDO ESTRITO

- ✓AFASTAMENTO DE SIGILO BANCÁRIO
- ✓AFASTAMENTO DE SIGILO TELEMÁTICO
- ✓TÉCNICA DE BUSCA E APREENSÃO

INVESTIGAÇÕES AO LONGO DO TEMPO

- ✓ **GERAÇÃO I** – foco no ciclo do conhecimento: prevalência da **ANÁLISE**
- ✓ **GERAÇÃO II** – prevalência da **EXPLORAÇÃO**: aproveitamento de oportunidades (ondas de operações)
- ✓ **GERAÇÃO III** – prevalência da **AÇÃO**: criação de oportunidades e de mais ação

CRIMES DE ALTA TECNOLOGIA

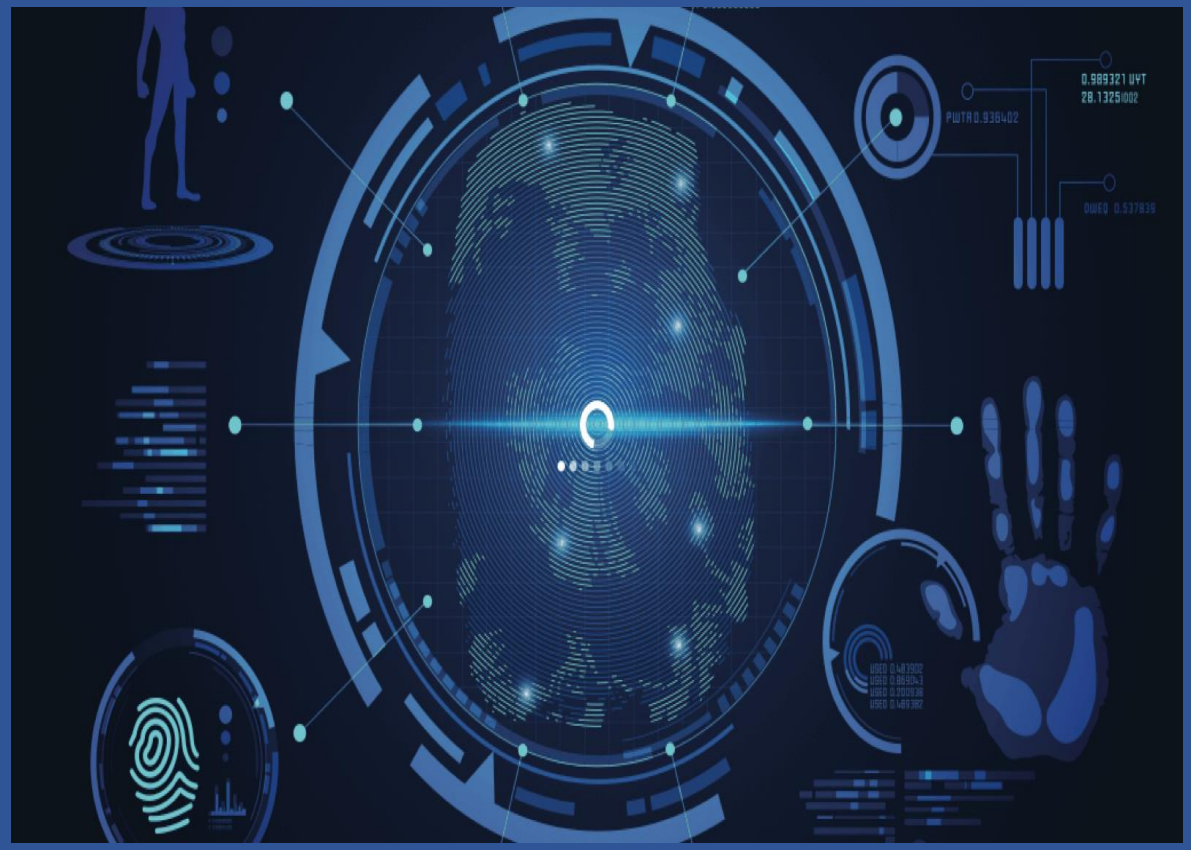
Invasão de dispositivos por meio de malwares

- ✓ VÍRUS
- ✓ BOTS / BOTNETS
- ✓ BANKER
- ✓ RANSOMWARE

PRESERVAÇÃO DE EVIDÊNCIA CIBERNÉTICA

RANSOMWARE

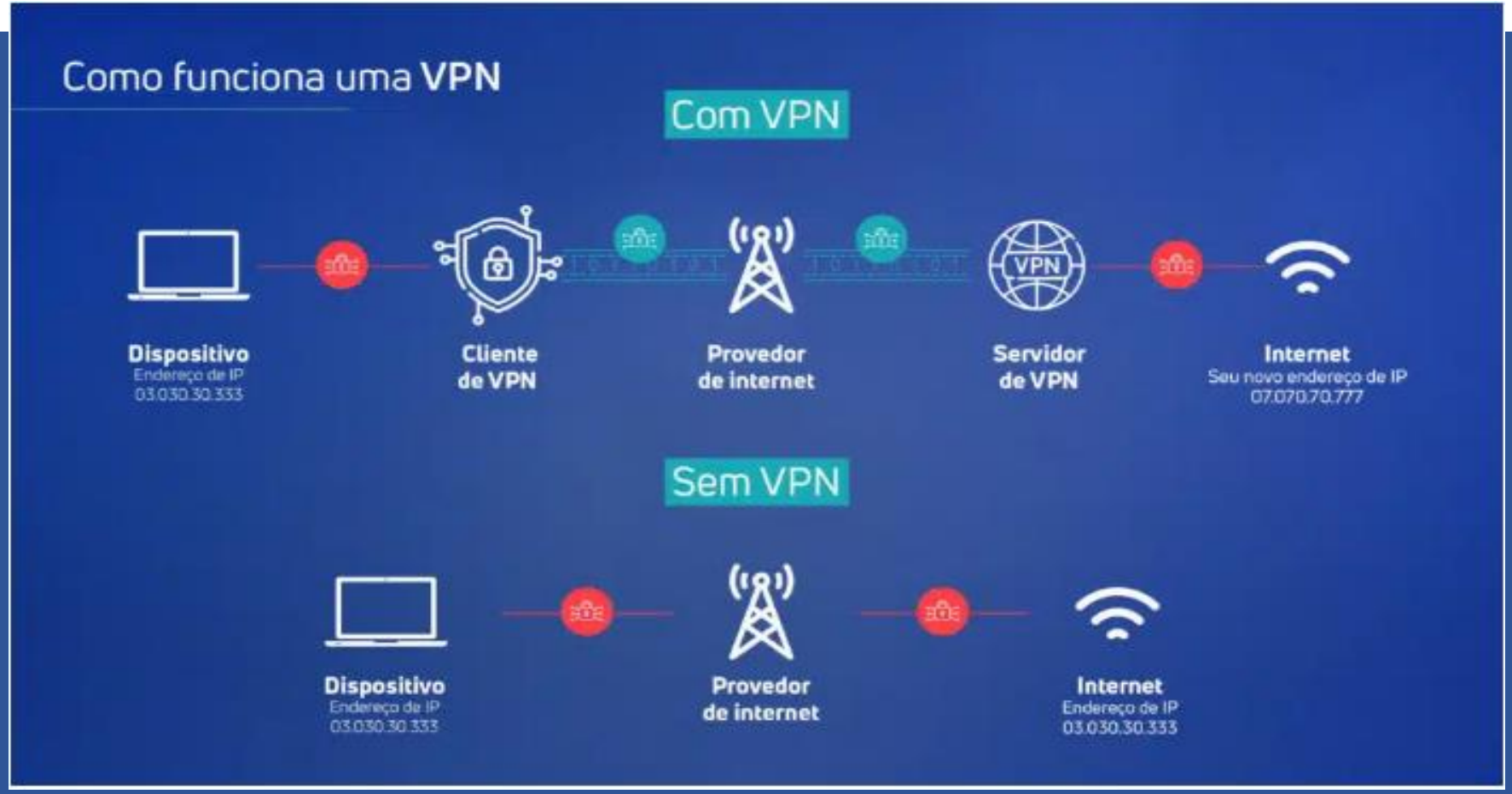
- ✓ Memória Flash - Dump
- ✓ Obtenção IP
- ✓ Uso VPN



Jurisdição e Privacidade

A jurisdição influencia a forma como um serviço de VPN aborda questões de privacidade. Os principais serviços de VPN são baseados em países que não estão associados à vigilância em massa. As leis de dados também favorecem as VPNs localizadas nesses países. Muitos provedores de VPN de elite, como o **ExpressVPN**, são acompanhados por com uma política rígida de não registro, garantindo o máximo de privacidade.

Técnicas de Anonimização



CASO ATAQUE RANSOMWARE

- ✓ **CRIPTOGRAFIA DE DADOS**
- ✓ **EXFILTRAÇÃO DE DADOS**
- ✓ **NOTA DE RESGATE**

PRIMEIROS PASSOS NO ATAQUE

1. Disparo de artifício malicioso
2. Vítima cai na engenharia social
3. Atacante coleta credenciais
4. Escalada de privilégios → A.D.

ESCALADA DE PRIVILÉGIOS

1. **USUÁRIO** - apenas faz uso dos recursos de um computador. Não pode instalar programas no computador que utiliza;

2. **ADMINISTRADOR LOCAL** - tem poder total sobre a máquina que utiliza, podendo instalar programas, mas não possui poder de administrador em outras máquinas do domínio;

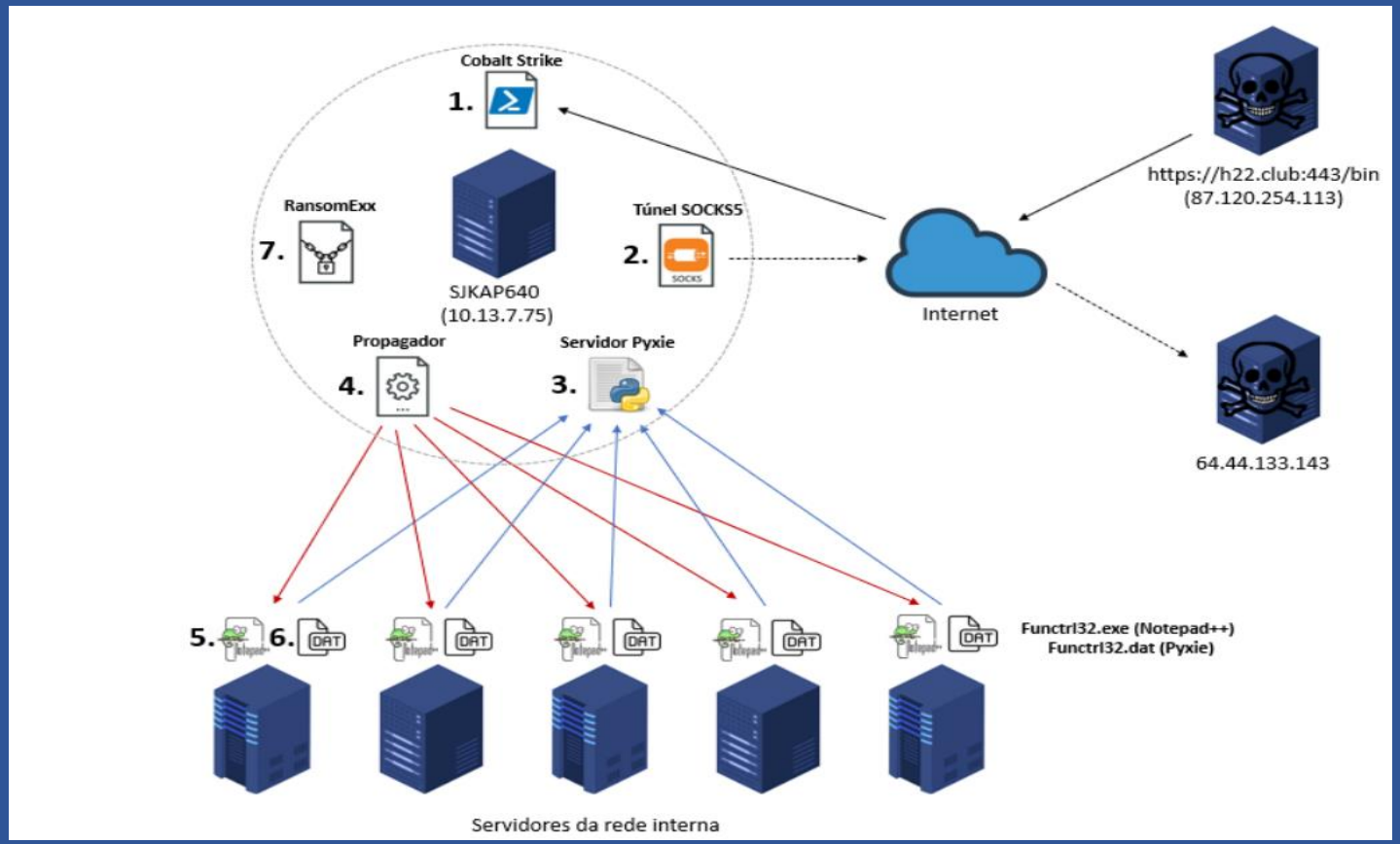
3. **ADMINISTRADOR DE DOMÍNIO** - pode fazer qualquer coisa dentro do domínio Windows. Tem acesso completo a todos os recursos.

CASO ATAQUE RANSOMWARE

EXAME PERICIAL - ENGENHARIA REVERSA

Quem está operando?

Quem desenvolveu?



COOPERAÇÃO

- **Jurídica Internacional**
- **Policial**
- **Convenção de Budapeste**

OBRIGADO!