

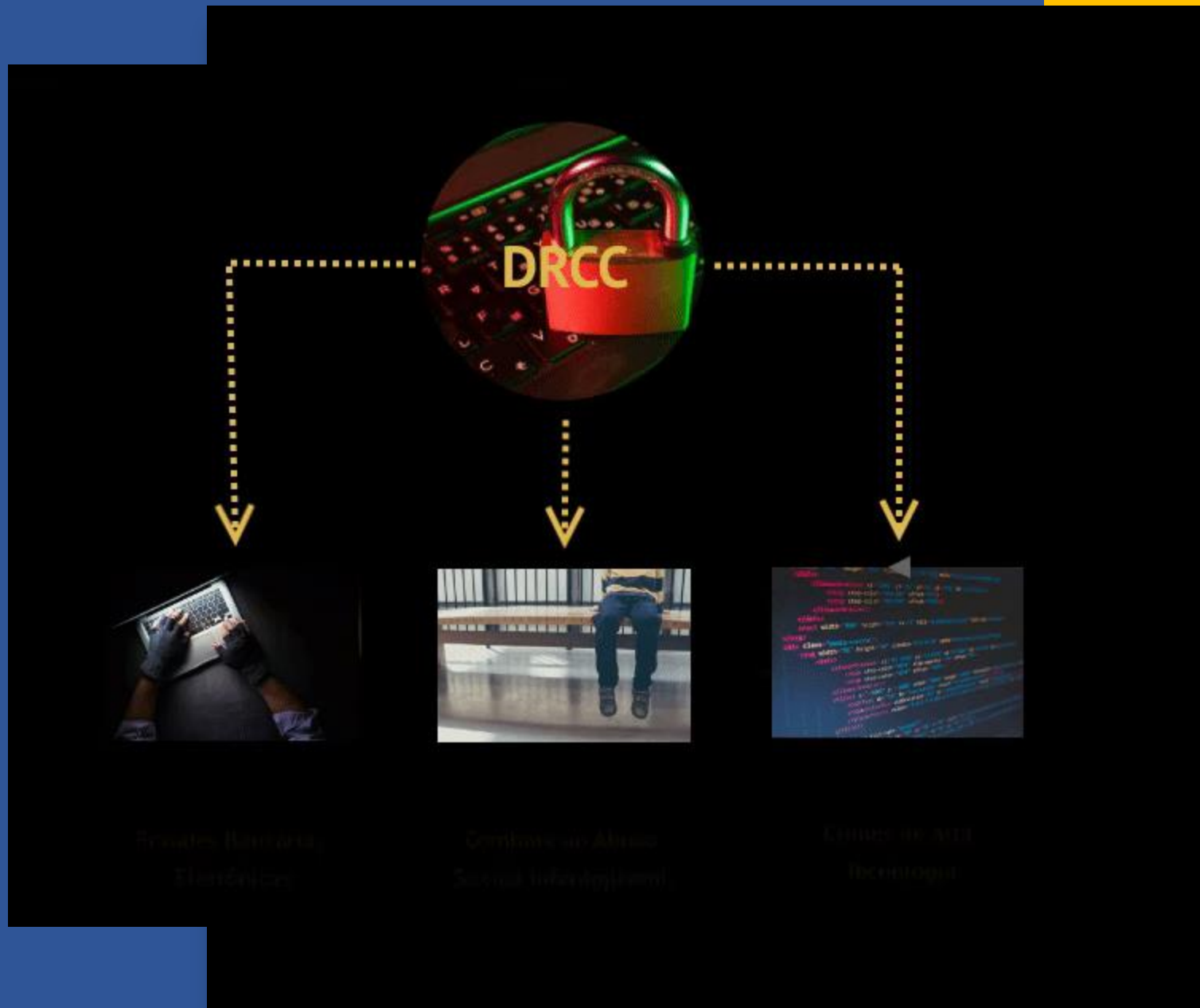


Vestígios eletrônicos, investigação e a perícia nos crimes cibernéticos

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

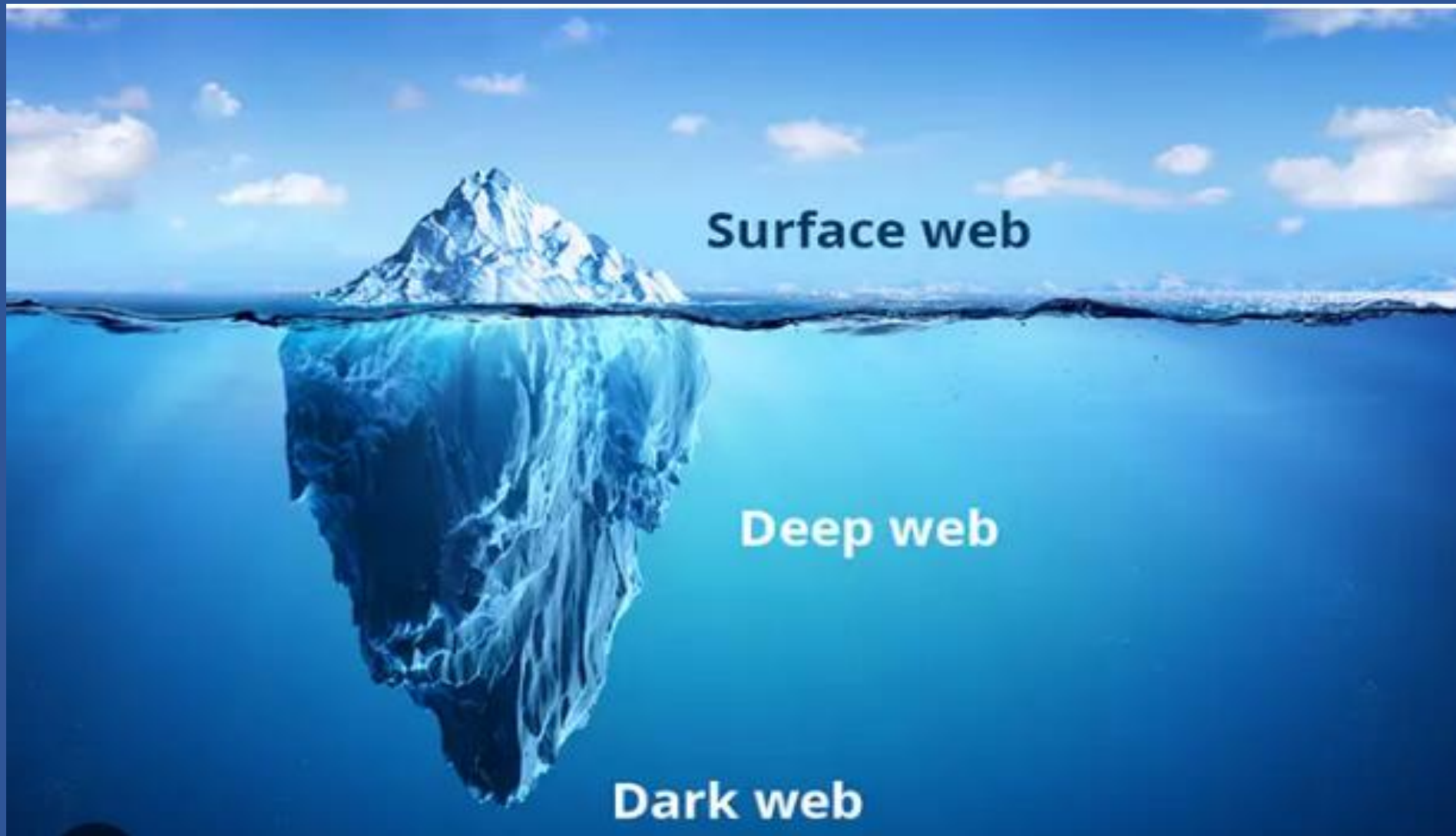




VESTÍGIOS EM CRIMES RELACIONADOS AO ABUSO SEXUAL INFANTOJUVENIL

PRIVACIDADE ou **CONIVÊNCIA?**







VESTÍGIOS EM FRAUDES BANCÁRIAS ELETRÔNICAS

O GLOBO 80 anos

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

Tony Vieira/Diário do Nordeste



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.

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 par-

cialmente. 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**



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

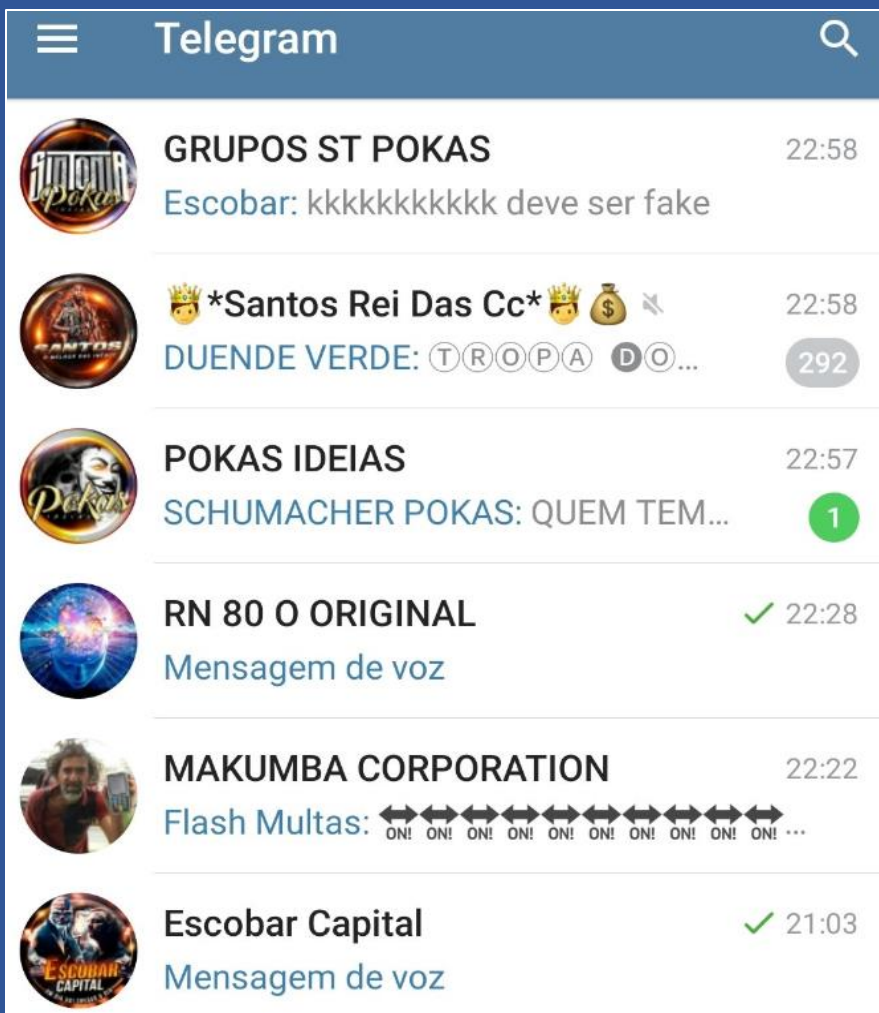
**Mais de 1,7 milhão de golpes com Pix foram
aplicados em 2022, mostra levantamento**

Estudo realizado por fintech também mostra golpes mais recorrentes, confira

**FRAUDES
BANCÁRIAS
ELETRÔNICAS**



MODO DE OPERAÇÃO



Peba Pks (5511937039639@s.whatsapp.net)

PebaBR, [valores atualizados AGORA COM MATERIAL COLHIDO DIARIAMENTE * \$\$*PEBA *LISTA.DE.CPF.E.SENHA * *100 k de db CPF e senha de.6 numericas100k=500* *CPF E SENHA DE-4 100100100/500 *Lista.cpf.numerica e A álpha numéricas =100k=500\$ *COMPLETA* *lista CPF e Senha de (8)=20k=300\$•50k=600numericas* *100 100*senha de 8 chegou material novo colhido no dia *lista de emeil e senha 100 k de emeil 300reais * * vem no melhor é correto * *A MAIS BARATA DA NET* *NA QUANTIDADE TÊM VALOR MAIS BARATO AINDA* *Garanta Seu Tranpo com a melhor dB da Net* *qualidade.pokas ideia. 7de elite* o melhor é 100 da net

2021-04-01 11:50:40 -03:00

TOP CC
Banner

AS MELHORES INFOCC FULL DADOS DA NET NOME + CPF

*LOTE MIX	
10CC-----	R\$ 350
20CC-----	R\$600
30CC-----	R\$ 750

*** UNIDADES**

BLACK-----	R\$ 150
INFINITE-----	R\$ 150
AMEX-----	R\$ 150
PLATINUM-----	R\$ 100
HIPER-----	R\$ 100
ELO-----	R\$ 70

ATENÇÃO NÃO GARANTO LIMITE DE SALDO ESQUEMA SITE APROVAÇÃO OU QUALQUER COISA RELATIVO. APENAS VENDO O MATERIAL.

MATERIAL VIRGEM * TROCAS EM 12H * NÃO TROCO INFO LIVE ENTREGA DE MATERIAL RÁPIDA

MATERIAL BATENDO 90% DE FULL DADOS E 80% DE QUALIDADE



MODO DE OPERAÇÃO

VENDA DE LOGIN E SENHA

VENDA DADOS

DADOS DE CARTÕES

PÁGINAS FALSAS

ENGENHARIA SOCIAL

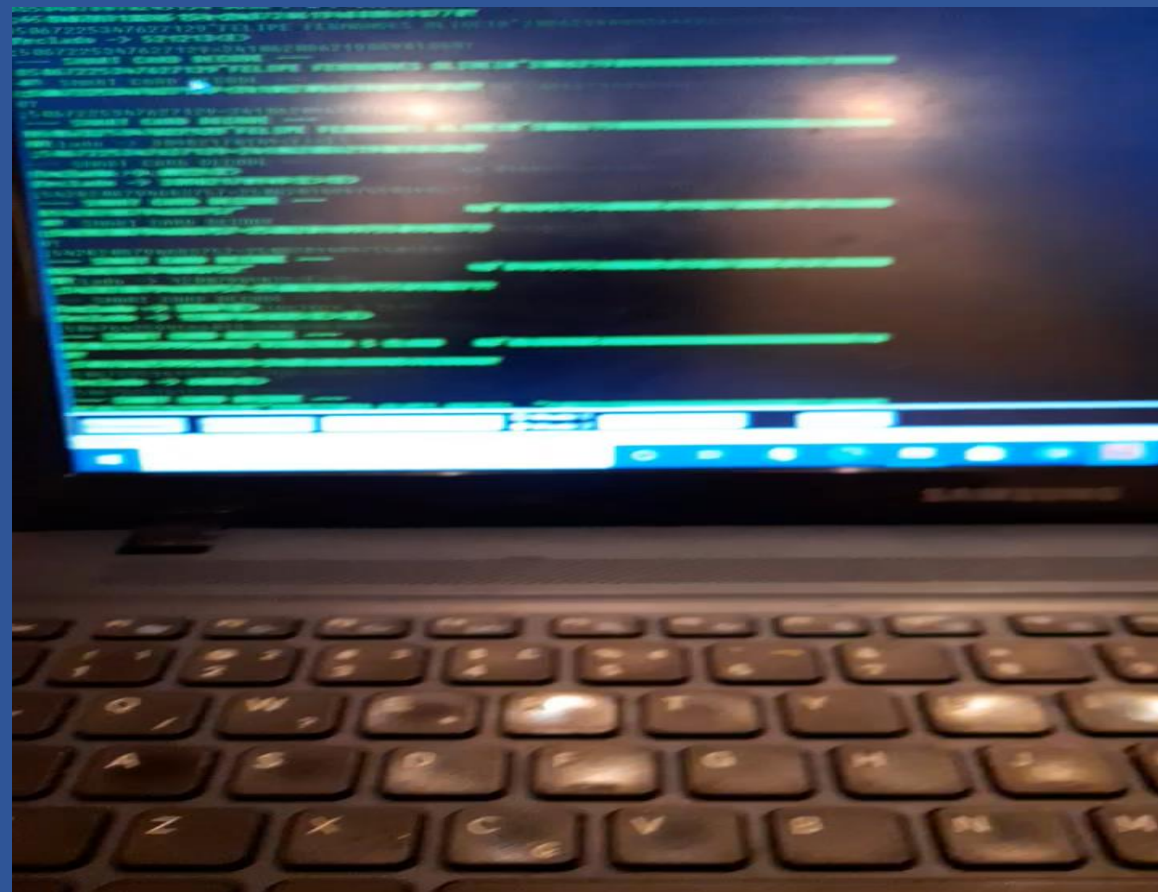
The screenshot shows the Itaú website's security check interface. At the top left is the Itaú logo. To the right, there are navigation links: "Acesso Cartões", "Sua Segurança", "Sobre", "Serviço", and "More". The main content area is titled "Consultar Segurança" with the subtitle "verifique acessos suspeitos no seu cartão". Below this, there is a short paragraph: "Para consultar e avaliar a segurança do seu cartão prossiga com todos os dados como costuma em sua conta." To the right of this text is a form titled "Verifique seus dados:" containing two input fields: "Número do Cartão:" and "Senha:". Below the fields is a grey button labeled "Acessar". At the bottom of the page, there is a footer with a breadcrumb trail: "Cartão de Crédito com as melhores vantagens | Itaú > Serviços | Itaúcard > Titular". The footer is organized into four columns: "Nossos produtos" (with links for cartões crédito, cartões de crédito, cartões de débito, cartões, cartões pré-pagos, cartões de crédito, cartões de crédito), "Itaú" (with links for redução de impostos, cartões, seguros, seguros de vida, seguros de vida, seguros de vida, seguros de vida), "Ajuda" (with links for manual de ajuda, cartões, cartões, cartões, cartões, cartões, cartões), and "Seja parte de Itaú" (with links for SAC 0800 724 1174, SAQUE 0800 875 0822, atendimento, atendimento). There is also a "acompanhe" section with social media icons and a "para mais" link.



OBTENÇÃO E COMÉRCIO DE DADOS

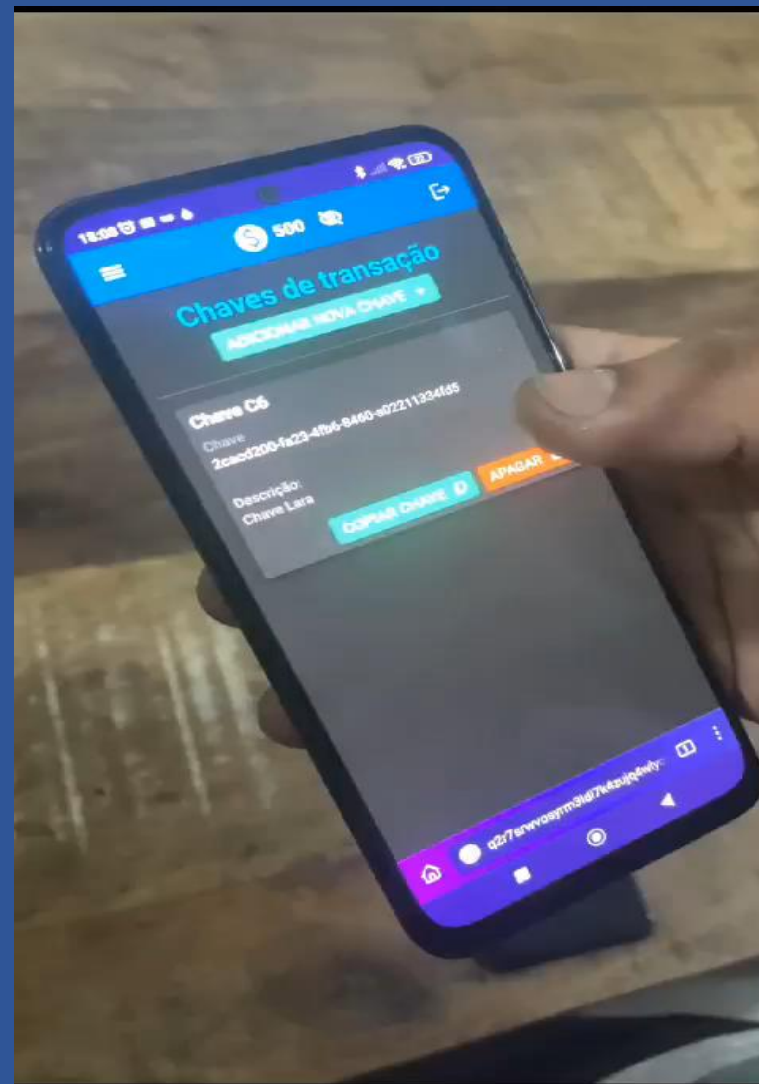
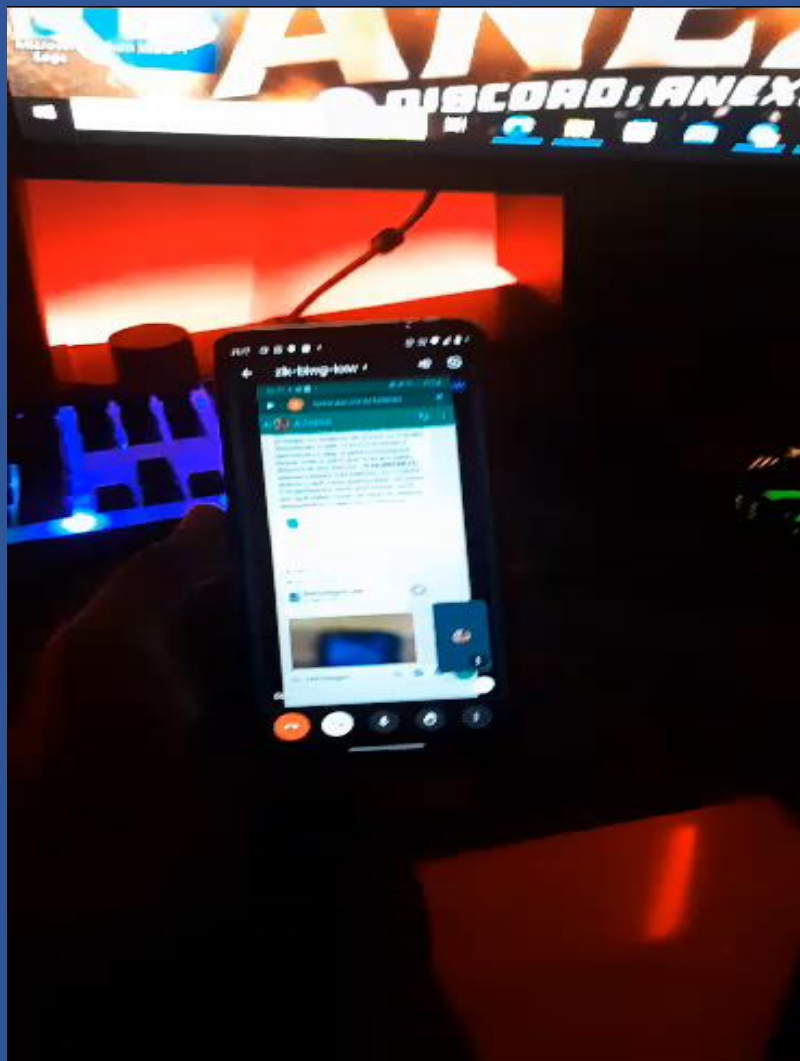
Dispositivo de clonagem instalados em maquinas

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.

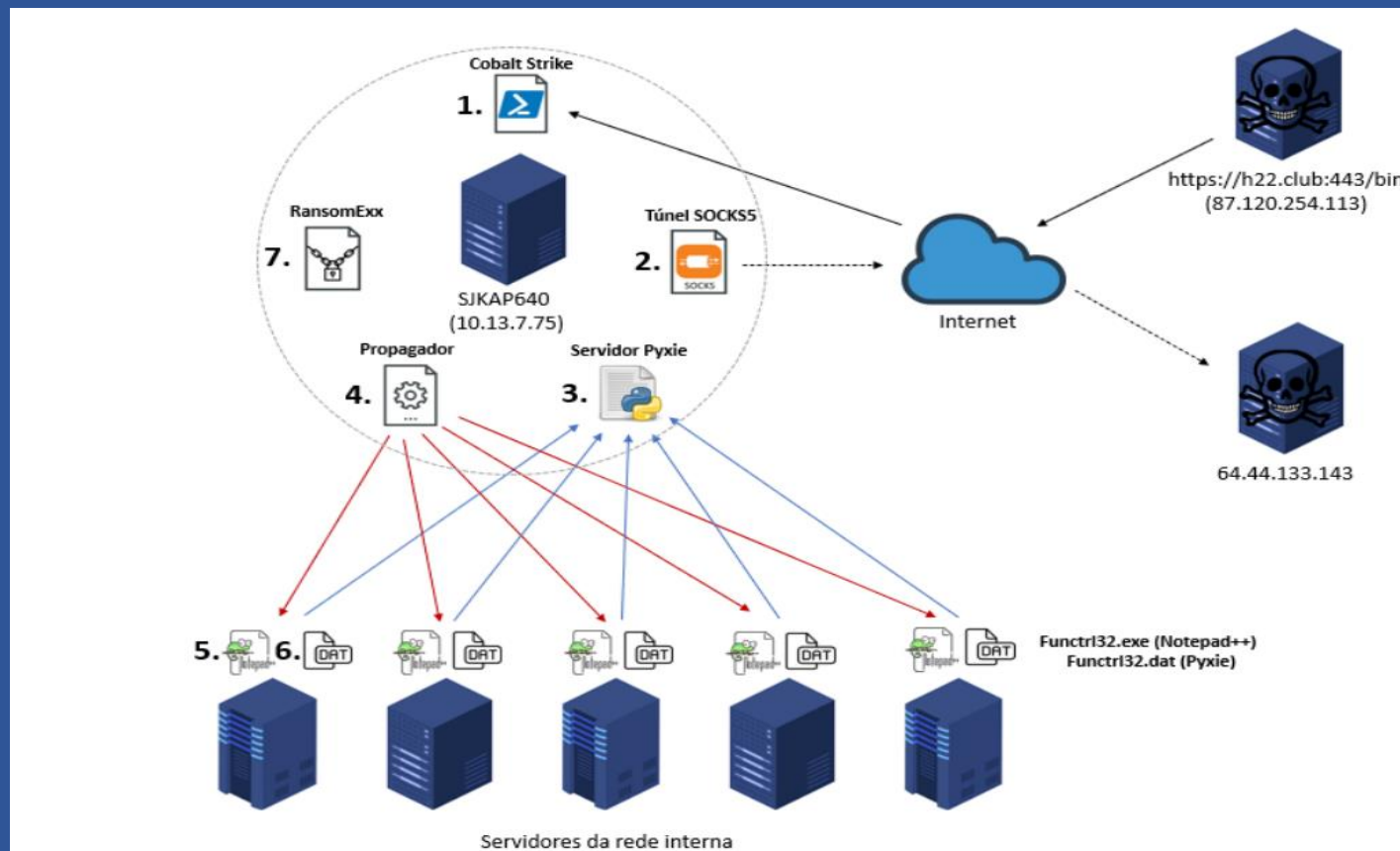


CASO ATAQUE RANSOMWARE

EXAME PERICIAL - ENGENHARIA REVERSA

Quem está operando?

Quem desenvolveu?





COOPERAÇÃO

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





OBRIGADO!