

ARQUITETURA DO CRIME

O papel dos painéis ilícitos na industrialização da fraude no Brasil

Quem sou

Francisco Neri

**Coordenador de Threat Hunting · Apura
Cybersecurity Intelligence**

Atuo em inteligência cibernética, threat hunting e investigação de ecossistemas ilícitos digitais, com foco em fraude, vazamentos de dados e infraestruturas ilícitas.

- Coordenador de Threat Hunting na Apura Cybersecurity Intelligence
- Coautor do livro OSINT do Zero à Investigação Profissional
- Pesquisador em fraude digital, OSINT e ecossistemas ilícitos
- Autor da linha de pesquisa sobre Arquitetura do Crime



TLP-CLEAR



Quando um vazamento termina?

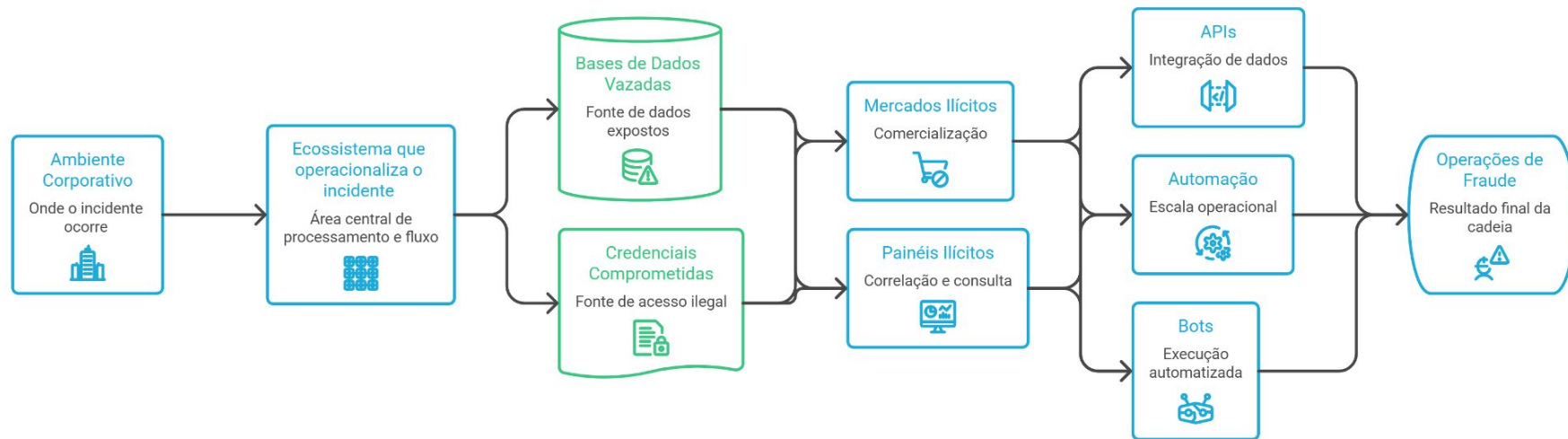


Ele não termina !

TLP-CLEAR

Ele muda de ecossistema

Como um incidente passa a integrar um ecossistema ilícito





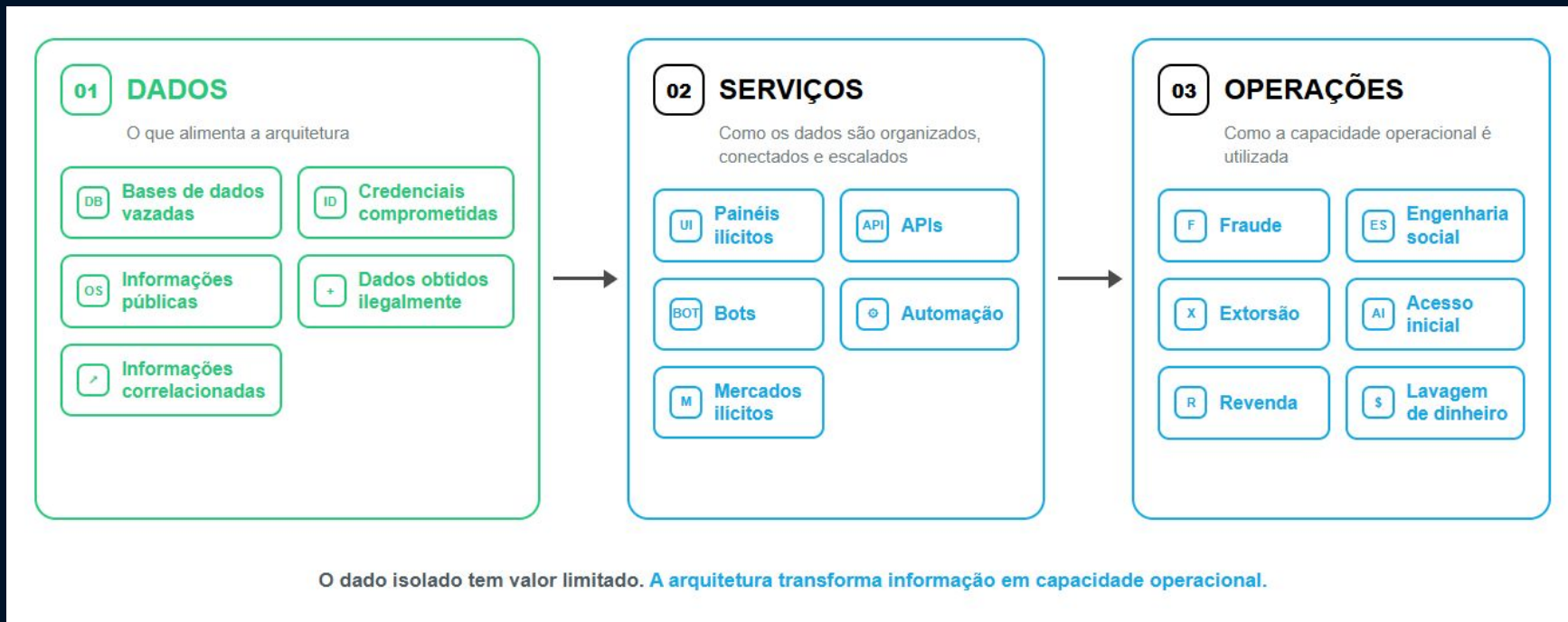
TLP-CLEAR

**Essa infraestrutura
tem nome.**

ARQUITETURA DO **CRIME**

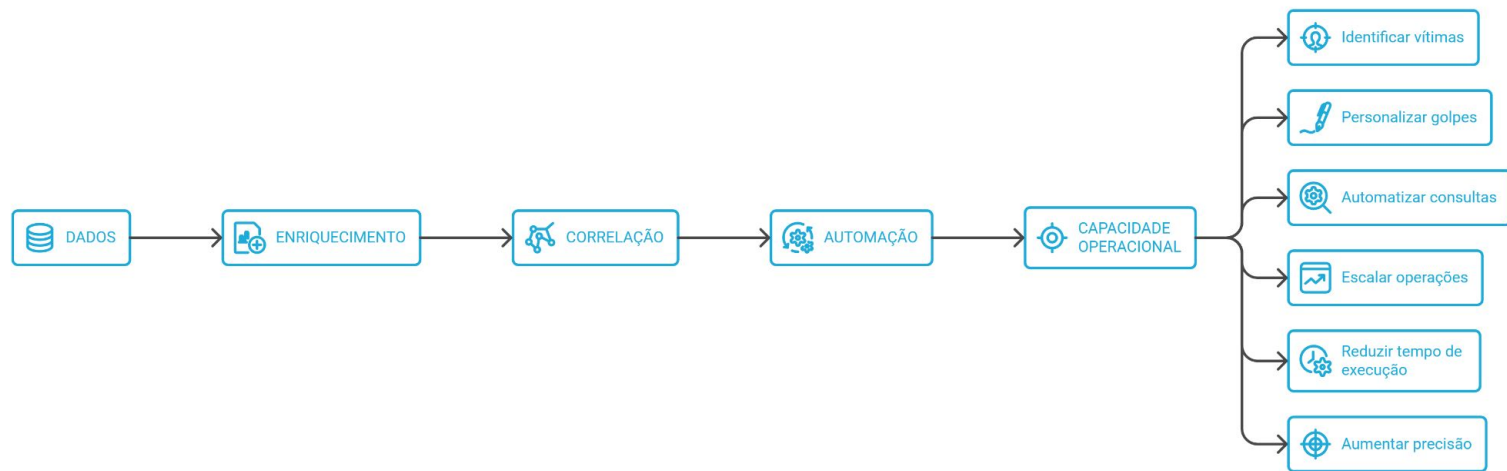
— • —
COMPREENDER PARA PREVENIR.
MAPEAR PARA ENFRENTAR.

Os três pilares da Arquitetura do Crime



O verdadeiro produto não é o dado

É a capacidade operacional construída sobre ele



O valor não está no dado.

Está na capacidade de transformá-lo em ação.



Um CPF isolado tem pouco valor. O verdadeiro valor surge quando ele é enriquecido, correlacionado e automatizado.

O ator malicioso não paga pelo dado em si; ele paga para reduzir esforço, ganhar contexto e receber uma capacidade operacional pronta para uso.

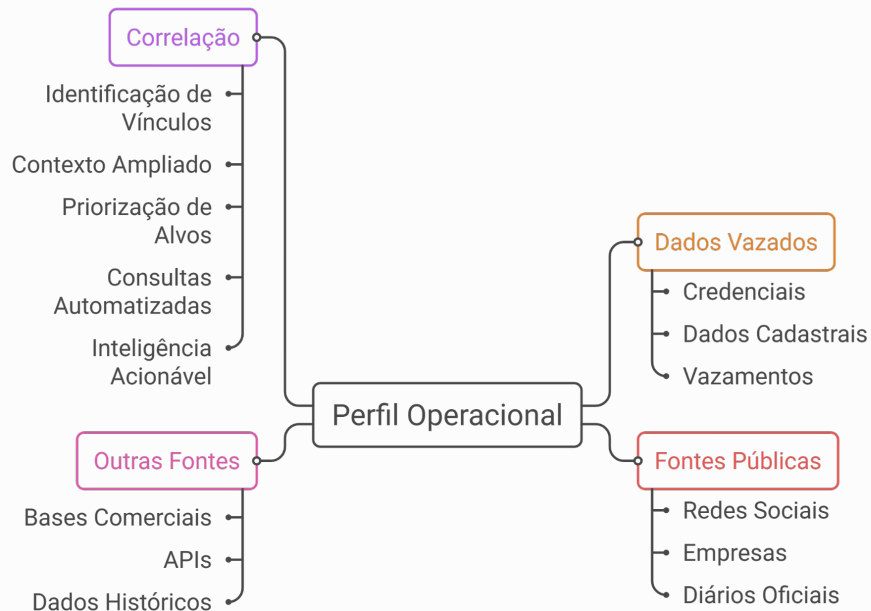
O impacto não é tecnológico.

É operacional.



A força está na correlação.

Nenhuma base de dados é suficiente por si só.



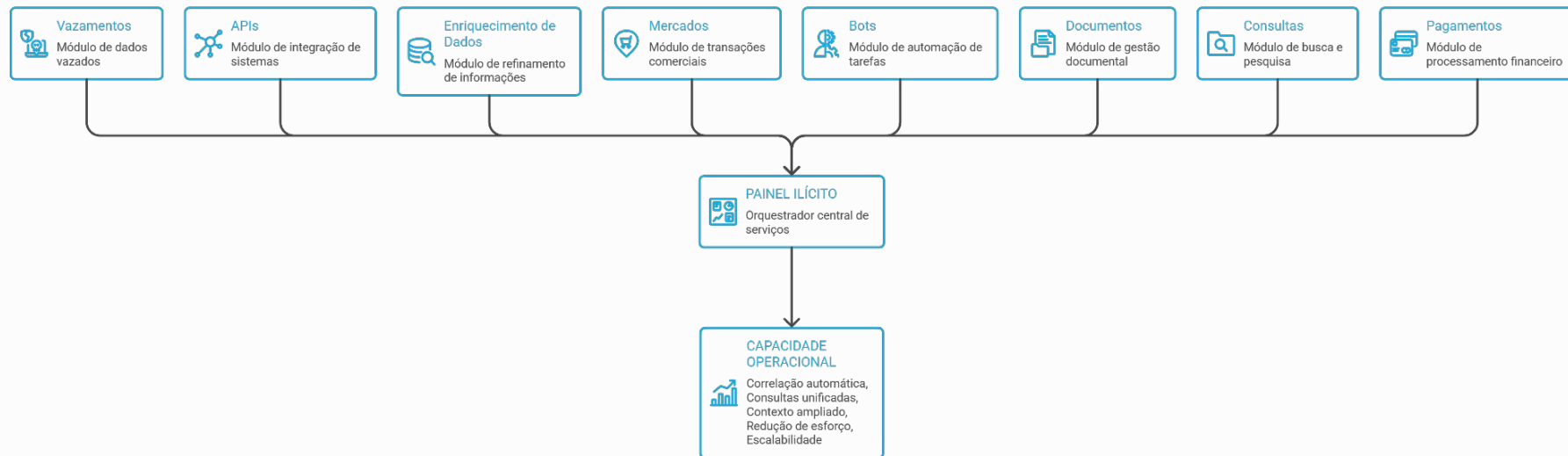
Mensagem

- Nenhum painel possui todas as respostas.
- O diferencial está na capacidade de integrar informações de diferentes origens.
- Um endereço encontrado em uma fonte, um telefone em outra, um veículo em uma terceira e um vínculo empresarial em uma quarta passam a formar um único contexto operacional.
- O ativo mais valioso não é a base de dados. É o mecanismo de correlação.

Quanto maior a capacidade de correlacionar dados,
maior a capacidade de compreender e explorar um
alvo.

Um painel nunca trabalha sozinho

O ecossistema é formado pela especialização e integração de serviços.



O diferencial competitivo não é possuir dados. É integrar serviços

O crime também possui uma cadeia de suprimentos.

Quando pensamos em fraude, normalmente imaginamos um criminoso sozinho, sentado em frente a um computador. Mas, ao longo das investigações, o que observamos é algo muito diferente. Existe uma cadeia de especialização.

Alguns atores obtêm os dados. Outros desenvolvem as plataformas. Outros integram serviços. Há quem comercialize acessos e há quem apenas execute a fraude. Cada um agrega valor em uma etapa específica. É exatamente esse modelo que permite escalar operações.



Da teoria para a prática

 CPF Consulta básica	 CPF PRO Dados completos	 Nome Busca por nome	 Nome Similar Busca aproximada	 RG Registro Geral	 Título Eleitor Dados eleitorais
 CNS Cartão Saúde	 Telefone Números cadastrados	 Email E-mails cadastrados	 CEP Endereços por CEP	 CEP Avançado Busca por endereço	 NIS Identificação Social
 Placa Veículos	 Placa Ghost Dados completos	 CNH Carteira Nacional	 Chassi Número do chassi	 Renavam Registro de Veículos	 Aposentado Dados previdenciários
 Hist. Funcionários Registro trabalhista	 Hist. Empregos Histórico trabalhista	 COVID-19 Vacinas e testes	 Desmascarador Revelação de dados	 Processos Judiciais	 Score Pontuação crédito
 Parentes Família	 Árvore Familiar Rede de parentes	 Chave PIX Consulta por chave	 Hist. Chave PIX Histórico por CPF	 CNPJ Dados empresariais	 Gerador Estado Dados por UF
 Gerador CBO	 Cloud URL	 Cloud Usuário	 Senha	 Mãe	 Pai



Painel



Configurações

Dashboard

Consulte dados através de nosso painel.



CPF

Consultando CPF
nacionalmente.



RG

Consultando RG
nacionalmente.



Nome

Consultando Nome
nacionalmente.



Pais

Consulte nome dos
filhos.



Telefone

Consultando Telefone
nacionalmente.



Foto

Consulte fotos através
do CPF ou Nome.



Veicular

Consulte placa, motor,
chassi ou radar.



Nascimento

Dados através da data
de nascimento.



Empresas

Consulte uma
empresa.



Vizinhos

Consulte vizinhos.



CEP

Consulte dados
através do CEP.



E-Mail

Consulte dados de
um e-mail.



Score

Consulte o score de
um cpf.



Radar(manutenção)

Consulte a localização
de um veículo.



Cns

Consulte dados pelo
cns.



Beneficios

Consulte beneficios
recebidos pelo cpf.



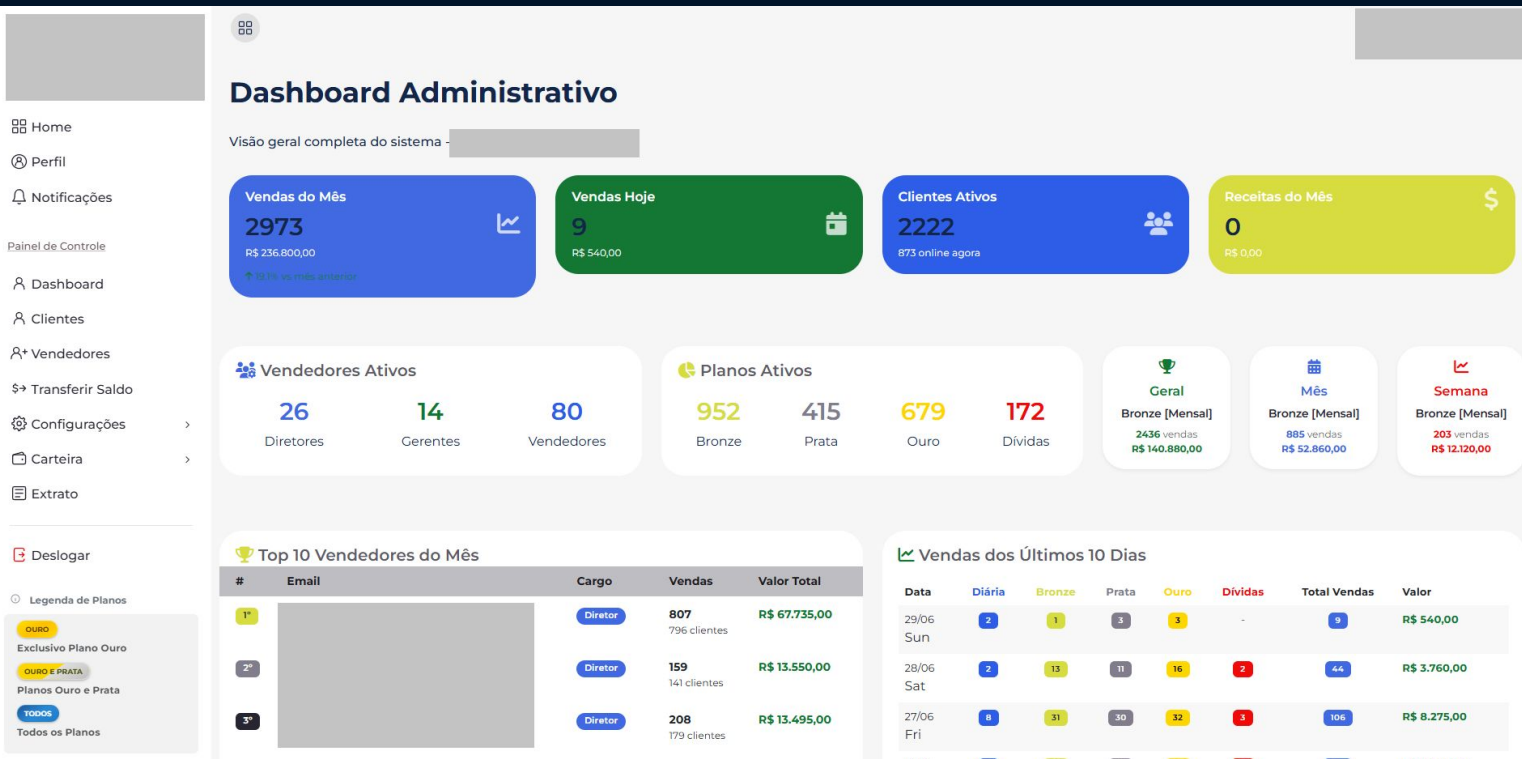
Armas

Consulte as armas
registradas pelo cpf.



Empregos

Consulte via cpf, onde
a pessoa já trabalhou.



Dados Completos

Veiculos

CNH

Ferramentas

Fotos

Empresarial

Registros Nacionais

Financeiro

Geradores

Especiais

🔍 Mais Utilizados

FACEBASE

FaceBase Mais Utilizado

2000 consultas restantes

FACEDATA

FaceData Mais Utilizado

998 consultas restantes

RECONHECIMENTO FACIAL

Reconhecimento Facial Online Mais Utilizado Novo

1000 consultas restantes

FOTOS SÃO PAULO

Fotos São Paulo Mais Utilizado

100 consultas restantes

BUSCA RADAR 2.0

Radar 2.0 (crédito normal) Mais Utilizado

10 consultas restantes

BUSCA RADAR

Radar Online Mais Utilizado Novo

3 consultas restantes

FOTO CNH NACIONAL

Foto CNH Nacional Online Mais Utilizado Novo

5 consultas restantes

MANDADOS

IMÓVEIS

NOME

BENS MÓVEIS

Análise de Inteligência

Padrões de movimentação identificados a partir de 22 passagens



PERÍODO



19

DIAS ATIVOS



Sexta

PICO: DIA



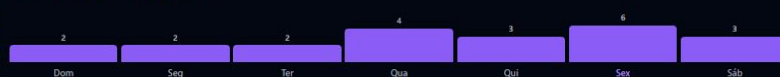
Tarde

PICO: HORÁRIO

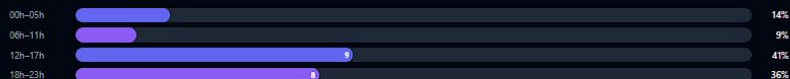
Locais mais frequentes

AM - MANAUS - AV. GOV. JOSE LINDOSO - SENT M12-M01 -> BOLA DO COROADO - 16°DIP	5x
AM - MANAUS - R. PEDRO DE ATAIDE - SENT M12-M06 -> R. 74 (AUTO ESCOLA LENE) - (6°DIP)	2x
AM - MANAUS - AV. CONSTANTINO NERY - SENT M12-M01 -> AV. ALVARO MAIA - 22°DIP	2x
AM - MANAUS - AV. JOSE ROMAO - SENT M01-M08 -> ESC. EST. ERNESTO PENAFORT (9°DIP)	2x
AM - MANAUS - AV. DES. JOAO MACHADO - SENT M02-M12 -> RODOVIARIA - (12°DIP)	2x
AM - MANAUS - AV. JORN. UMBERTO CALDERARO FILHO - SENT M01-M12 -> CSU PARQUE 10 - 23°DIP	1x
AM - MANAUS - AV. CONSTANTINOPLA - SENT -> POSTO DE GASOLINA (ATEM)	1x
AM - MANAUS - AV GOV JOSE LINDOSO - SENT -> BOLA DO COROADO	1x

Frequência por dia da semana



Faixa de horário



Locais mais frequentados por dia da semana

Seg	2 passagens	Ter	2 passagens	Qua	4 passagens	Qui	3 passagens
1. AM - MANAUS - AV. CEL. FERREIRA DE ARAUJO - SENT -> AV. CODAIAS - (3°DIP)	1x	1. AM - MANAUS - AV. DR. THEOMARIO PINTO DA COSTA - SENT M012-M02 BOLA DAS LETRAS - DOM PEDRO - (22°DIP)	1x	1. AM - MANAUS - AV. DES. JOAO MACHADO - SENT M02-M12 -> RODOVIARIA - (12°DIP)	2x	1. AM - MANAUS - AV. CONSTANTINO NERY - SENT M12-M01 -> AV. [REDACTED]	2x
2. AM - MANAUS - AV. GOV. JOSE LINDOSO - SENT M12-M01 -> BOLA DO COROADO - 16°DIP	1x	2. AM - MANAUS - AV. GOV. JOSE LINDOSO - SENT M12-M01 -> BOLA DO COROADO - 16°DIP	1x	2. AM - MANAUS - AV. GOV. JOSE LINDOSO - SENT -> BOLA DO COROADO	1x	2. AM - MANAUS - AV. GOV. JOSE LINDOSO - SENT M12-M01 -> BOLA DO COROADO - 16°DIP	1x
				3. AM - MANAUS - AV. LAGUNA - SENT -> AV. CORONEL TEIXEIRA	1x		
Sex	3 passagens	Sáb	3 passagens	Dom	2 passagens		
1. AM - MANAUS - [REDACTED] (ATEM)	1x	1. AM - MANAUS - AV. JORN. UMBERTO CALDERARO FILHO - SENT M01-	1x	1. AM - MANAUS - R. PEDRO DE ATAIDE - SENT M12-M06 -> R. 74 (AUTO ESCOLA LENE) - (6°DIP)	1x		
2. AM - MANAUS - ESCOLA LENE - (	1x	2. AM - MANAUS - AV. GOV. JOSE LINDOSO -	1x	2. AM - MANAUS - AV. JOSE ROMAO - SENT M01-M08 -> ESC. EST. ERNESTO PENAFORT (9°DIP)	1x		
3. AM - MANAUS - ERNESTO PENAR	1x	3. AM - MANAUS - AV. MAX TEIXEIRA -	1x				

O que isso muda para um CSIRT?

A resposta ao incidente não termina na contenção.

Modelo tradicional

- ✗ Conter o incidente
- ✗ Remover artefatos
- ✗ Corrigir vulnerabilidades
- ✗ Restaurar o ambiente

Visão ampliada

- ✓ Monitorar o reaproveitamento dos dados
- ✓ Identificar novos vetores de exploração
- ✓ Acompanhar o enriquecimento das informações
- ✓ Alimentar CTI e Hunting

O objetivo deixa de ser apenas conter o incidente. Passa a ser compreender sua evolução.

Mensagem:

Tradicionalmente, encerramos um incidente quando a causa raiz foi tratada.

Mas quando há exposição de dados, o incidente continua existindo em outro ecossistema.

A partir desse momento, a pergunta deixa de ser 'o atacante ainda está na minha rede?' e passa a ser 'como esses dados estão sendo utilizados?'



Cinco ideias para levar desta palestra

1. Um vazamento não termina quando é divulgado.
2. Dados isolados possuem baixo valor operacional.
3. A correlação transforma dados em capacidade operacional.
4. A fraude em larga escala depende de um ecossistema especializado.
5. Compreender esse ecossistema fortalece a resposta e a prevenção.

Conclusão

Quando um vazamento termina?

Ele não termina

Ele muda de ecossistema

Compreender a Arquitetura do Crime é ampliar a capacidade de defesa antes que os dados expostos sejam transformados em novas operações

— ENCERRAMENTO

Obrigado!

Arquitetura do Crime

O papel dos painéis ilícitos na
industrialização da fraude no Brasil

Francisco Neri

Threat Hunting · Cyber Threat Intelligence · OSINT



eu.0moura.io

Aponte a câmera para continuar

Apresentação, artigos, pesquisas e projetos disponíveis no QR Code.

14º Fórum Brasileiro de CSIRTs

TLP-CLEAR



MIAMI

2 S. Biscayne Boulevard
Suite 245
Zip Code: 33131
Phone/FAX: (305) 921 9562

SÃO PAULO

Av. Paulista 2421
Ed. Bela Paulista, 1º andar
CEP: 01310-300
Telefone: (11) 5504 1966

BRASÍLIA

SHN Quadra 1 Lote A Bloco A
Ed. Le Quartier, 14º andar
CEP: 70701-010
Telefone: (61) 3255-1245

TLP-CLEAR



bttNEO
elite