1 Ameaças

1.1 Metodologia de modelagem de ameaças

Este anexo tem o objetivo de auxiliar o leitor a ter o pleno entendimento sobre a modelagem das ameaças contidas neste documento. Para isto serão apresentados todos os componentes de uma ameaça, a metodologia de qualificação utilizada, e por fim, como interpretar o passo a passo do atacante estruturado no grafo de ameaças.

Composição de uma ameaça

Uma ameaça é composta por três componentes base: *Atacante*, *Mecanismo* e *Ativo*. Estes três componentes são representados graficamente por círculos, compondo a trinca da ameaça.

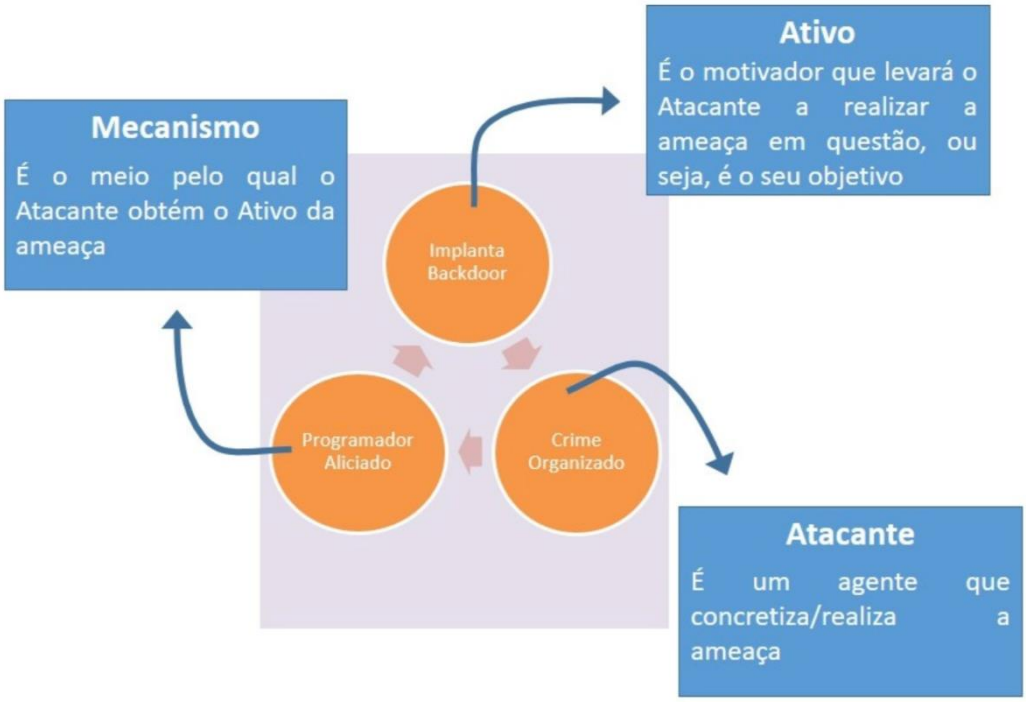


Figura 1 - Detalhamento dos três componentes base

Esta trinca deve ser interpretada da seguinte maneira: *"O Atacante através de um Mecanismo, obtém o Ativo"*, por exemplo: *"O Crime Organizado através de um Programador Aliciado, Implanta uma Backdoor"*. Desta forma a ameaça é uma representação gráfica de um cenário de ataque.

Atacante

O *Atacante* é o agente que realiza ações maliciosas com a motivação de obter um retorno (mesmo que as vezes indireto) financeiro em 99% dos casos.

Mecanismo

O *Mecanismo* é o meio pelo qual o *Atacante* obtém o *Ativo da Ameaça*. Na maioria das ameaças, o *Atacante* utiliza como *Mecanismo* recursos computacionais, mas também pode vir a utilizar recursos humanos. Os meios utilizados são inúmeros, e não estão limitados aos sistemas, abuso de processos da empresa, aliciamento de funcionários. Podendo também utilizar de mais de um meio dependendo do objetivo.

Ativo

O *Ativo* é o motivador que levará o *Atacante* realizar a ameaça em questão, ou seja, é o seu objetivo. O *Ativo* obtido em uma ameaça pode se tornar um *Mecanismo* em outra ameaça.

Composição

A ameaça é descrita através de três componentes base e de componentes de risco. Todos os componentes são dispostos na ficha da ameaça.

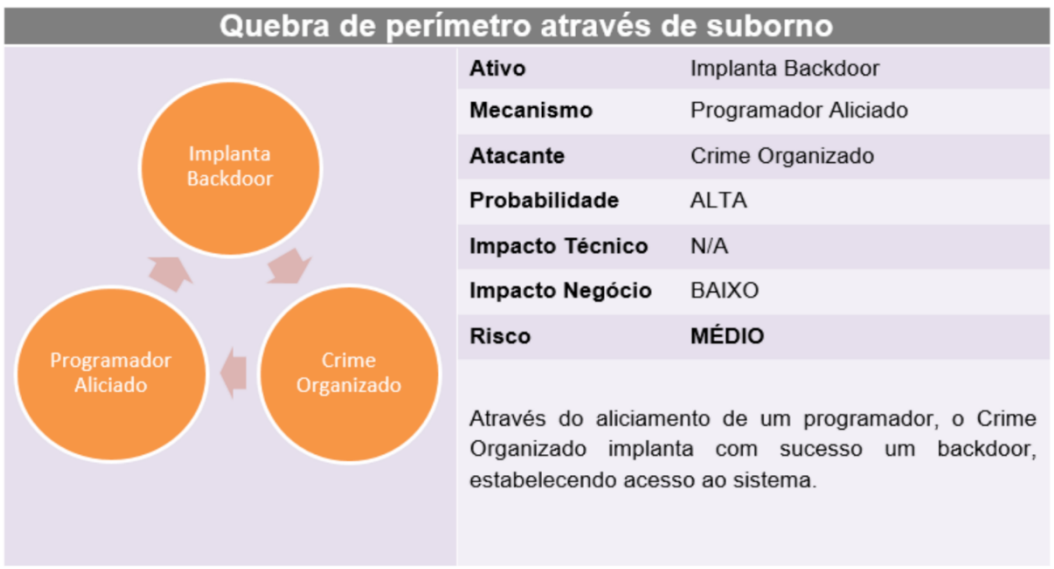


Figura 2 - Exemplo da ficha de uma ameaça

Além dos componentes base, os itens *Nome da ameaça* e *Descrição da ameaça* também são importantes para compreender a ameaça.

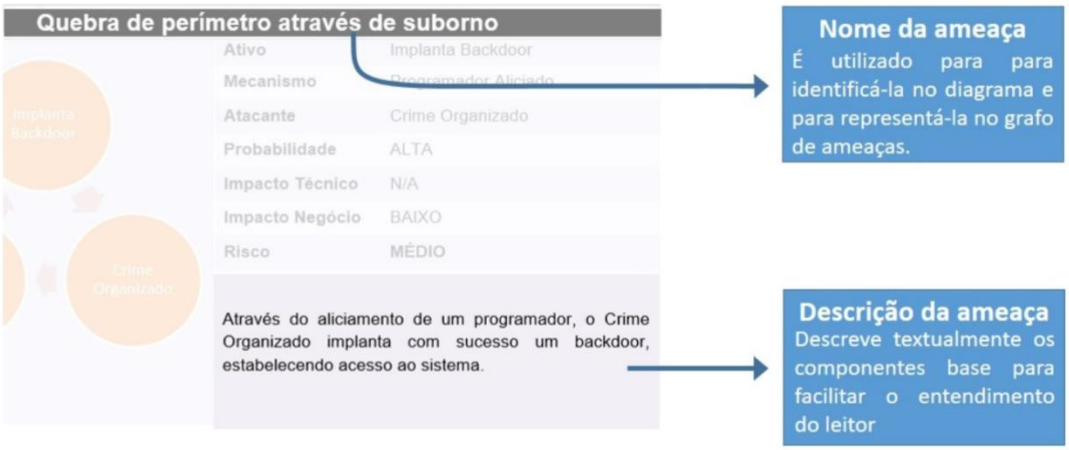


Figura 3 - Detalhamento da ficha da ameaça

Nome da ameaça

O *Nome da ameaça* é o menor resumo de uma ameaça. É utilizado para identificá-la e também para representá-la no *Grafo de ameaças*.

Descrição da ameaça

A *Descrição da ameaça* descreve textualmente os componentes base para facilitar o entendimento do leitor. Em alguns casos, insere alguns detalhes que não são possíveis de representar na trinca.

Grau de risco

A representação gráfica dos componentes base é colorida de acordo com o grau de risco da ameaça, que é obtido através da qualificação do mesmo.

A qualificação é calculada com base em três aspectos: *Probabilidade*, *Impacto Técnico* e *Impacto de Negócio*.

Os aspectos de risco (*Probabilidade*, *Impacto Técnico* e *Impacto de Negócio*) e a metodologia para obter o grau de risco estão descritos no subtópico *Qualificação de ameaças*.

Qualificação de uma ameaça

A metodologia utilizada para qualificação das ameaças é baseada na metodologia da OWASP (OWASP *Risk Rating Methodology*), que pode ser acessada através do endereço https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

Cada um dos três aspectos de risco é estimado através da média de fatores. Cada fator assume um valor numérico entre zero (0) e nove (9).

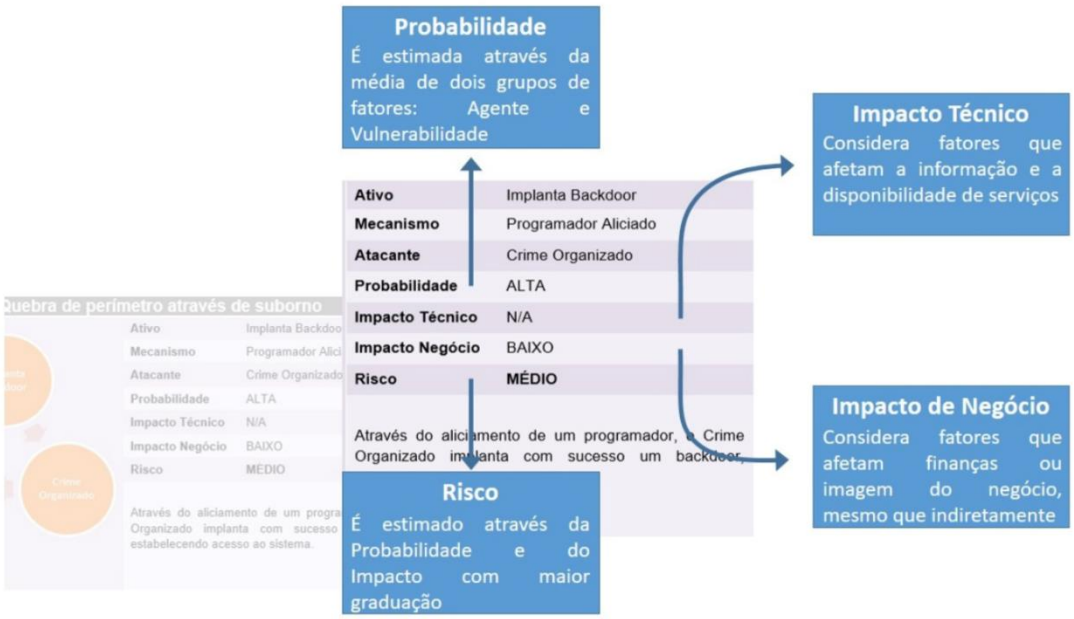


Figura 4 - Detalhamento dos aspectos de risco

Probabilidade

A *Probabilidade* é estimada através da média de dois grupos de fatores: *Agente da ameaça*, que possui fatores relacionados ao *Atacante*; e *Vulnerabilidade*, que possui fatores sobre a descoberta e a exploração da vulnerabilidade pelo *Atacante*.

Impacto Técnico e Impacto de Negócio

O *Impacto Técnico* é um aspecto que considera fatores que afetam a informação e disponibilidade de serviços. Enquanto o aspecto *Impacto de Negócio* considera fatores que afetam as finanças ou a imagem do negócio, mesmo que indiretamente.

Ambos os aspectos de *Impacto* também são estimados através da média de fatores. Entretanto, a média de ambos é comparada, e o *Impacto* que apresentar o maior valor é selecionado para calcular o grau do risco.

Tanto os aspectos de *Probabilidade* quanto os aspectos de *Impacto* são compostos por quatro fatores, conforme pode ser observado abaixo.

	Probabilidade		Impacto	
	Agente	**Vulnerabilidade**	**Impacto Técnico**	**Impacto de Negócio**
Fatores	Nível de habilidade	Facilidade em ser descoberta	Perda de confiabilidade	Dano financeiro
	Motivação	Facilidade em ser explorada	Perda de integridade	Dano de reputação
	Oportunidade	Experiência	Indisponibilidade	Falta de aderência a normas
	Tamanho	Detecção de intruso	Perda de rastreabilidade	Violação de privacidade

Tabela 1 - Lista de fatores de cada aspecto

A média de cada aspecto resulta em uma graduação, conforme abaixo:

- Caso a média seja maior que zero (0) e menor que três (3), o aspecto é qualificado como Baixo;
- Quando a média é maior que três (3) e menor que seis (6), o aspecto é qualificado como Médio;
- Se a média é maior que seis (6) e menor ou igual a nove (9), o aspecto é qualificado como Alto.

Risco

O grau de risco é obtido através da correlação entre a graduação da *Probabilidade* e do *Impacto*, refletido na matriz de risco abaixo.

Impacto	ALTO	**Médio**	**Alto**	**Crítico**
	MÉDIO	**Baixo**	**Médio**	**Alto**
	BAIXO	**Nota**	**Baixo**	**Médio**
		BAIXA	MÉDIA	ALTA
	Probabilidade			

Tabela 2 - Matriz de correlacionamento para obtenção do grau de risco

Cada grau de risco é representado por uma cor que sinaliza a sua criticidade. A cor que representa o risco é replicada na trinca da ameaça e também no *Grafo de ameaças*.

Grau de risco	Cor
Crítico	
Alto	
Médio	
Baixo	
Nota	

Tabela 3 - Relação de grau de risco e cor

Grafo de ameaças

No *Grafo de ameaças*, uma ameaça é representada através de um retângulo. Assim como na representação dos componentes base, a ameaça no *Grafo de ameaças* possui uma coloração de acordo com seu grau do risco.

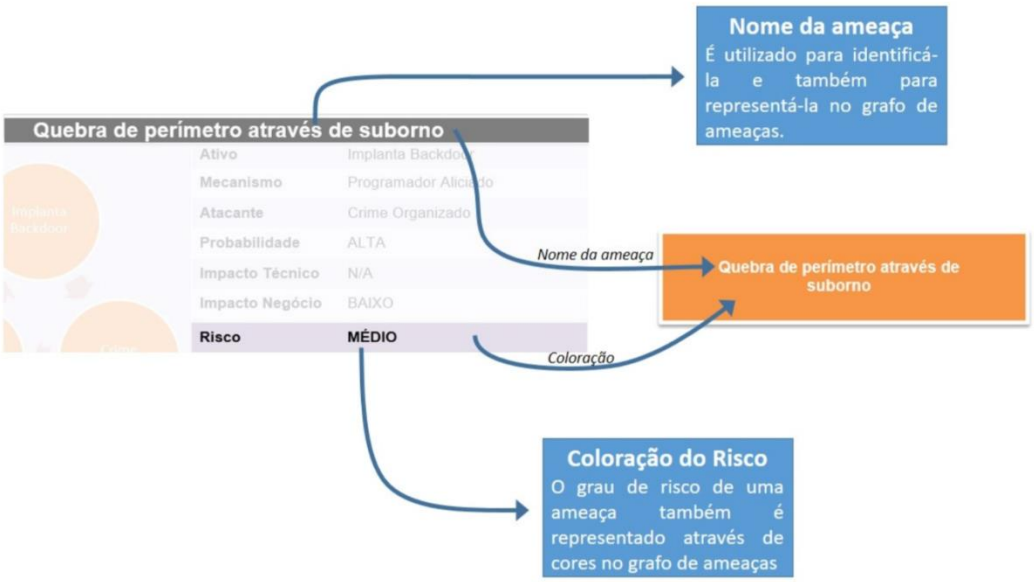


Figura 5 – Detalhamento da representação da ameaça no grafo

Através do *Grafo de ameaças* é possível observar a sequência de passos que um *Atacante* realiza até obter o resultado final do ataque, que em geral, é representado pelo último nível do grafo.

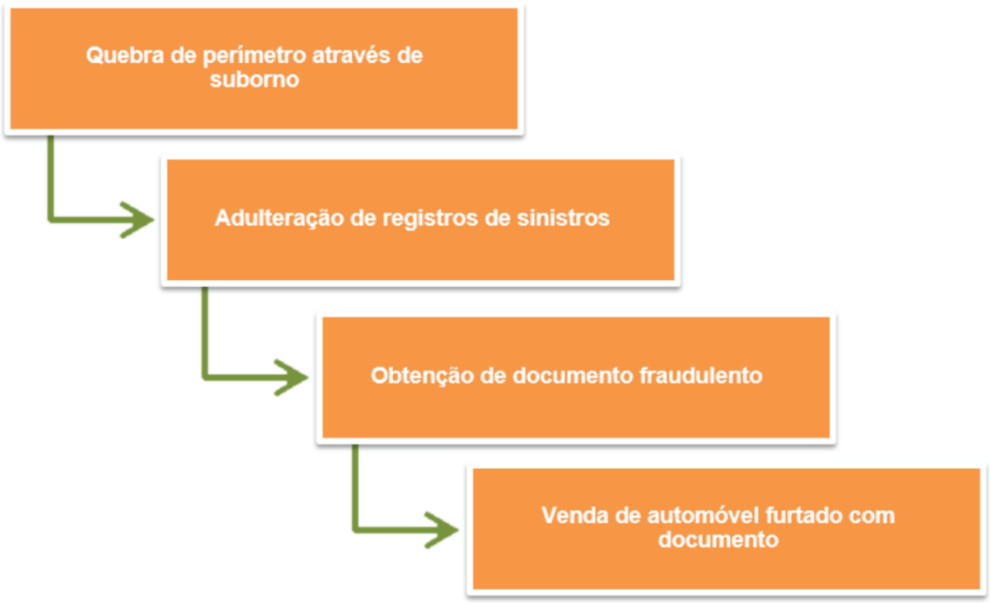


Figura 6 - Exemplo de um grafo de ameaças

Em cada ameaça o *Atacante* visa obter um *Ativo*, que é o seu objetivo, mas o *Ativo* obtido pode não ser o objetivo final. Uma vez obtido, o *Ativo* de uma ameaça pode se tornar um *Mecanismo* em outra ameaça. Por esse fato as ameaças podem ser encadeadas.

O encadeamento das ameaças é representado no *Grafo de ameaças* através de setas verdes.

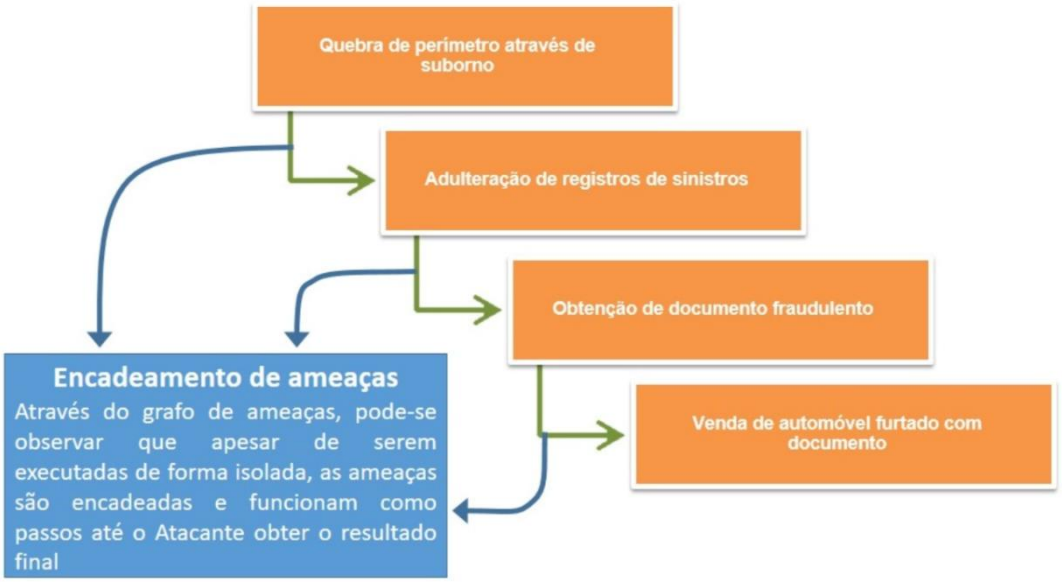


Figura 7 - Explicação sobre o encadeamento de ameaças

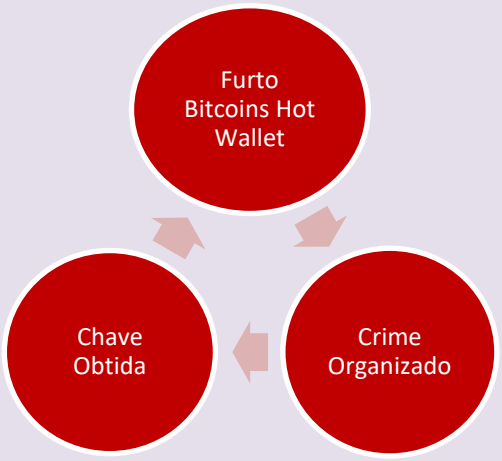
O grafo também possibilita visualizar que uma ou várias ameaças iniciais podem ser utilizadas pelo *Atacante* para obter o resultado final de um ataque.

Figura 8 –Grafo de ameaças com mais de uma ameaça inicial

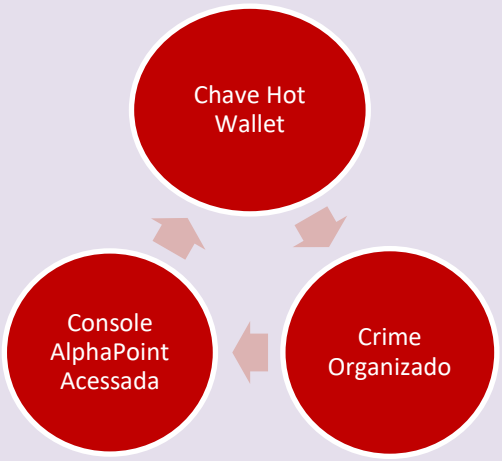
Em conjunto com a coloração de risco, a visualização das ameaças em um grafo visa aumentar a eficácia da priorização de medidas de segurança, bem como análise de causa raiz.

1.2 Modelagem de ameaças

Crime Organizado: Grupos transacionais, nacionais ou locais altamente centralizados e geridos por criminosos, que pretendem se envolver em atividades ilegais, geralmente com o objetivo de lucro monetário. Esse tipo de atacante geralmente dispõe bastantes recursos, de tempo e dinheiro.

Furto de bitcoins localizados no AlphaPoint (hot wallet)	
	
Ativo	Furto Bitcoins Hot Wallet
Mecanismo	Chave Obtida
Atacante	Crime Organizado
Probabilidade	ALTA
Impacto Técnico	BAIXO
Impacto Negócio	ALTO
Risco	**CRÍTICO**
Em posse da chave privada da hot wallet, o Crime Organizado obtém controle sobre a hot wallet da EXCHANGE no AlphaPoint, e transfere os bitcoins para uma wallet sob seu controle.	

Obtenção da chave da hot wallet via console AlphaPoint



Ativo	Chave Hot Wallet
Mecanismo	Console AlphaPoint Acessada
Atacante	Crime Organizado
Probabilidade	ALTA
Impacto Técnico	BAIXO
Impacto Negócio	ALTO
Risco	**CRÍTICO**

Uma vez com acesso à console administrativa do AlphaPoint, o Crime Organizado obtém a chave privada referente à hot wallet.

Obtenção da chave da hot wallet por um colaborador EXCHANGE

Ativo	Chave Hot Wallet
Mecanismo	Colaborador XDEX
Atacante	Crime Organizado
Probabilidade	MÉDIA
Impacto Técnico	MÉDIO
Impacto Negócio	ALTO
Risco	**ALTO**

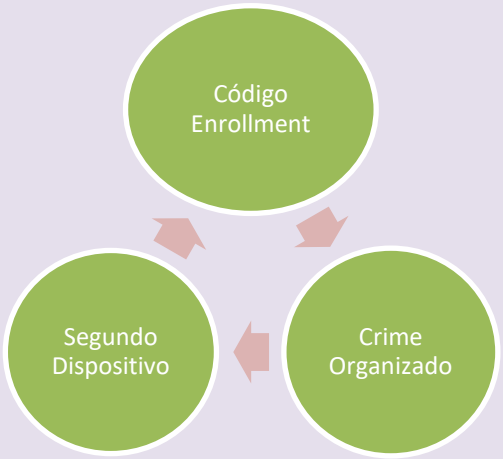
Ao “atacar” um colaborador da EXCHANGE com acesso à chave privada da hot wallet, o Crime Organizado obtém a mesma. Por “atacar” entenda: sequestrar, aliciar, comprometer dispositivos, etc.

Obtenção do 2FA do usuário por captura do seed

Ativo	Obtenção 2FA
Mecanismo	Seed Capturado
Atacante	Crime Organizado
Probabilidade	BAIXA
Impacto Técnico	MÉDIO
Impacto Negócio	ALTO
Risco	**MÉDIO**

Ao capturar o seed de um usuário, o Crime Organizado obtém acesso ao 2FA do mesmo.

Captura do código de enrollment do usuário



Ativo	Código Enrollment
Mecanismo	Segundo Dispositivo
Atacante	Crime Organizado
Probabilidade	BAIXA
Impacto Técnico	BAIXO
Impacto Negócio	MÉDIO
Risco	**BAIXO**

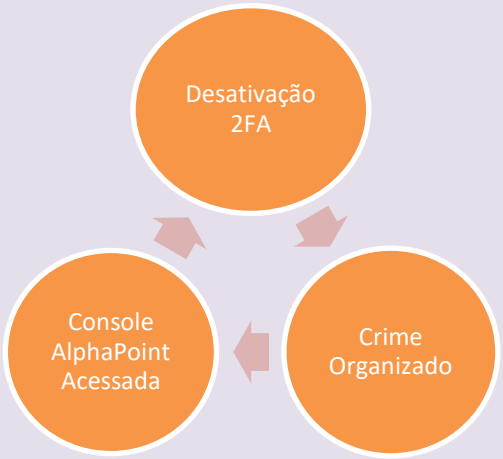
Ao adicionar um segundo dispositivo à conta do usuário no Sentinel, o Crime Organizado é capaz de capturar o código de enrollment do 2FA.

*Desativação fraudulenta do 2FA do usuário

Ativo	Desativação 2FA
Mecanismo	Aliciamento
Atacante	Crime Organizado
Probabilidade	ALTA
Impacto Técnico	MÉDIO
Impacto Negócio	BAIXO
Risco	**ALTO**

Ao aliciar um colaborador do time de atendimento da EXCHANGE, o Crime Organizado consegue a desativação do 2FA do usuário.

*Desativação fraudulenta do 2FA do usuário



Ativo	Desativação 2FA
Mecanismo	Console AlphaPoint Acessada
Atacante	Crime Organizado
Probabilidade	MÉDIA
Impacto Técnico	MÉDIO
Impacto Negócio	BAIXO
Risco	**MÉDIO**

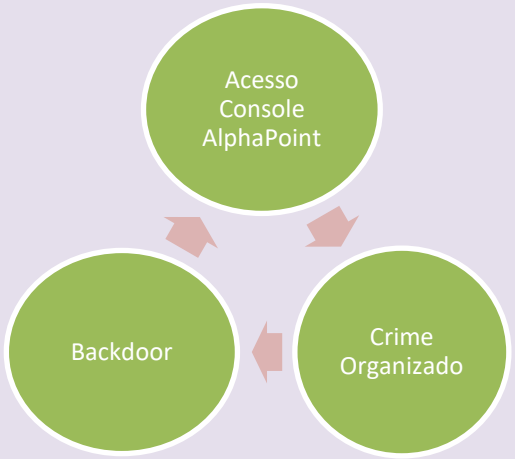
Uma vez com acesso à console administrativa do AlphaPoint, o Crime Organizado é capaz de desativar o 2FA do usuário.

*Acesso à console do AlphaPoint por aliciamento

Ativo	Acesso Console AlphaPoint
Mecanismo	Aliciamento
Atacante	Crime Organizado
Probabilidade	ALTA
Impacto Técnico	MÉDIO
Impacto Negócio	BAIXO
Risco	**ALTO**

A partir do aliciamento de um colaborador da área de TI ou de suporte, o Crime Organizado obtém acesso à console administrativa do AlphaPoint.

*Acesso à console do AlphaPoint via backdoor



Ativo	Acesso Console AlphaPoint
Mecanismo	Backdoor
Atacante	Crime Organizado
Probabilidade	BAIXA
Impacto Técnico	MÉDIO
Impacto Negócio	MÉDIO
Risco	**BAIXO**

Usando suas influências, o Crime Organizado inclui uma backdoor em algum componente interno utilizado na console administrativa, comprometendo o acesso à mesma.

Acesso à console do AlphaPoint por credencial vazada

Ativo	Acesso Console AlphaPoint
Mecanismo	Credencial de Acesso
Atacante	Crime Organizado
Probabilidade	MÉDIA
Impacto Técnico	MÉDIO
Impacto Negócio	MÉDIO
Risco	**MÉDIO**

Em posse de uma credencial vazada (ou obtida de alguma outra forma), o Crime Organizado obtém acesso à console administrativa do AlphaPoint.

Extorsão EXCHANGE através de IRPF de cliente vazado

Ativo	Extorsão
Mecanismo	IRPF Vazado
Atacante	Crime Organizado
Probabilidade	ALTO
Impacto Técnico	MÉDIO
Impacto Negócio	ALTO
Risco	**CRÍTICO**

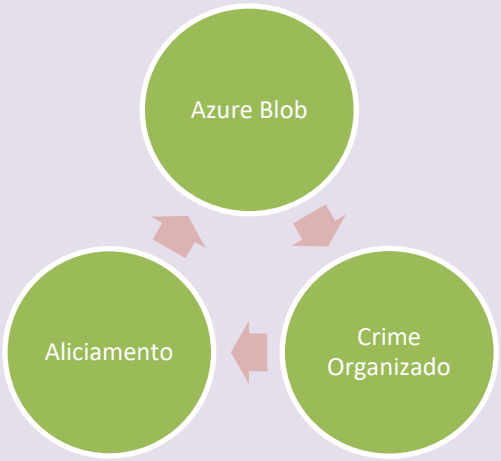
Por meio de um lote de documentos de IRPF vazados, o Crime Organizado extorque a EXCHANGE para não tornar público o vazamento.

Furto de IRPF através do Azure Comprometido

Ativo	IRPF
Mecanismo	Azure Comprometido
Atacante	Crime Organizado
Probabilidade	ALTO
Impacto Técnico	MÉDIO
Impacto Negócio	MÉDIO
Risco	**ALTO**

Através do ambiente Azure comprometido, o Crime Organizado tem acesso a lotes de IRPFs de clientes.

Comprometimento de acesso Azure-blob através de aliciamento



Ativo	Azure Blob
Mecanismo	Aliciamento
Atacante	Crime Organizado
Probabilidade	MÉDIO
Impacto Técnico	BAIXO
Impacto Negócio	BAIXO
Risco	**BAIXO**

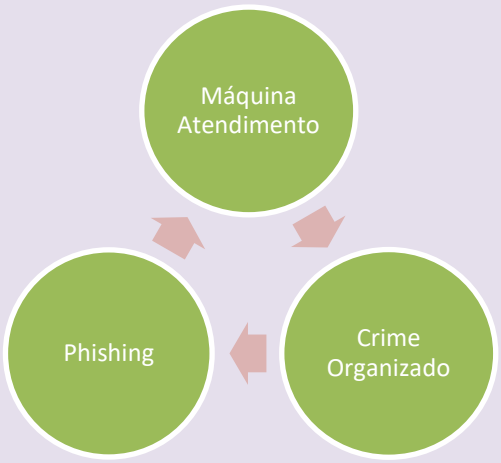
Através do aliciamento do staff de TI, o Crime Organizado obtém o acesso direto ao Blob do Azure que armazena os documentos da solução de trading de bitcoins, dentre eles o IRPF dos clientes.

Comprometimento de acesso Azure admin vazado

Ativo	Acesso Azure
Mecanismo	Admin Vazado
Atacante	Crime Organizado
Probabilidade	ALTO
Impacto Técnico	MÉDIO
Impacto Negócio	ALTO
Risco	**CRÍTICO**

Através do acesso administrativo à plataforma Azure, o Crime Organizado tem acesso a todos os dados e componentes da solução de trading de bitcoins, incluindo aos dados do IRPF de todos os clientes.

Comprometimento de máquina atendimento através de phishing



Ativo	Máquina Atendimento
Mecanismo	Phishing
Atacante	Crime Organizado
Probabilidade	MÉDIO
Impacto Técnico	BAIXO
Impacto Negócio	N/A
Risco	**BAIXO**

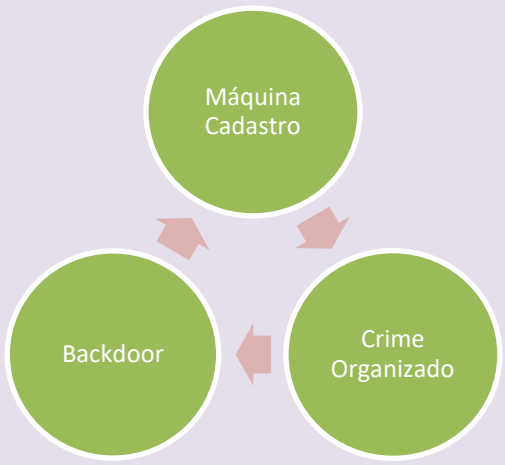
Através do envio de phishing para o atendimento, o Crime Organizado consegue comprometer a máquina do atendente, ganhando acesso a mesma.

Furto de IRPF através de máquina do cadastro comprometida

Ativo	IRPF
Mecanismo	Máquina Comprometida
Atacante	Crime Organizado
Probabilidade	ALTO
Impacto Técnico	MÉDIO
Impacto Negócio	MÉDIO
Risco	**ALTO**

Por meio da máquina do time de cadastro comprometida, o Crime Organizado obtém acesso direto aos documentos de IRPF que estiverem na própria máquina do analista.

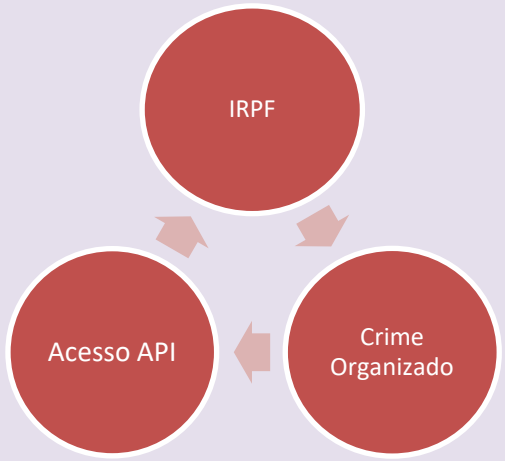
Comprometimento de máquina cadastro através de Backdoor



Ativo	Máquina Cadastro
Mecanismo	Backdoor
Atacante	Crime Organizado
Probabilidade	MÉDIO
Impacto Técnico	BAIXO
Impacto Negócio	N/A
Risco	**BAIXO**

Por meio do envio de PDFs (supostos IRPFs) maliciosos, o Crime Organizado infecta a máquina do time de cadastro, obtendo controle sobre a mesma.

Furto de IRPF através de acesso a API de cadastro comprometido



Ativo	IRPF
Mecanismo	Acesso API
Atacante	Crime Organizado
Probabilidade	ALTO
Impacto Técnico	MÉDIO
Impacto Negócio	MÉDIO
Risco	**ALTO**

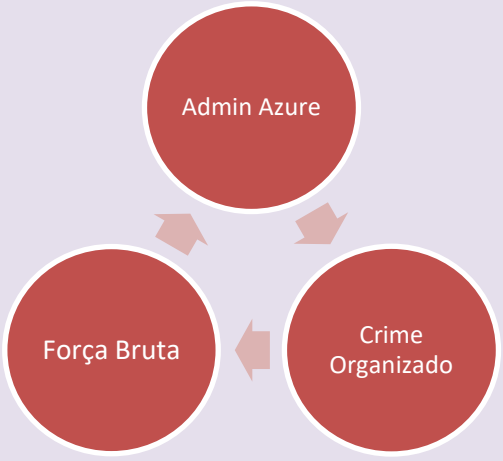
Por meio de acesso a API do KYC, o Crime organizado tem acesos indireto a toda a base de IRPFs de todos os clientes.

Comprometimento de acesso a API KYC através de máquina comprometida

Ativo	Acesso API
Mecanismo	Máquina Comprometida
Atacante	Crime Organizado
Probabilidade	MÉDIO
Impacto Técnico	BAIXO
Impacto Negócio	BAIXO
Risco	**BAIXO**

Através de uma máquina do time de Cadastro comprometida, o Crime Organizado obtém acesso a API de KYC (que dá acesso a toda a base de clientes e seus IRPFs).

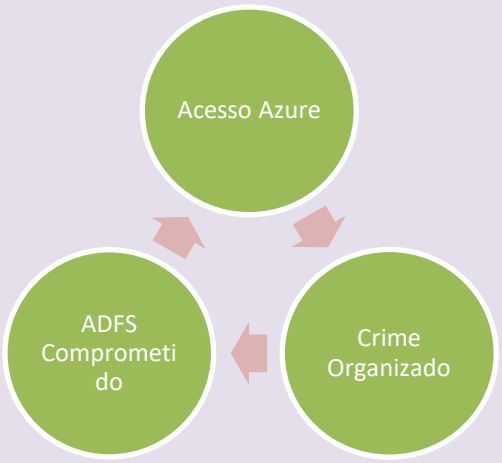
Comprometimento de acesso Azure através de ataque de força bruta



Ativo	Admin Azure
Mecanismo	Força Bruta
Atacante	Crime Organizado
Probabilidade	ALTO
Impacto Técnico	MÉDIO
Impacto Negócio	BAIXO
Risco	**ALTO**

Através de um ataque de força bruta (inúmeras tentativas de adivinhar a senha da conta admin do Azure), o Crime Organizado identifica a senha e ganha o acesso à plataforma.

Comprometimento de acesso Azure através do ADFS comprometido



Ativo	Acesso Azure
Mecanismo	ADFS Comprometido
Atacante	Crime Organizado
Probabilidade	MÉDIO
Impacto Técnico	BAIXO
Impacto Negócio	BAIXO
Risco	**BAIXO**

Através do acesso que o Crime Organizado possui sobre contas do ADFS, ele viabiliza o acesso a plataforma em si editando suas próprias permissões, garantindo seu acesso em nível administrativo no Azure.

Comprometimento de conta do ADFS através de aplicação

Ativo	Acesso Azure
Mecanismo	Aplicação
Atacante	Crime Organizado
Probabilidade	MÉDIO
Impacto Técnico	BAIXO
Impacto Negócio	BAIXO
Risco	**BAIXO**

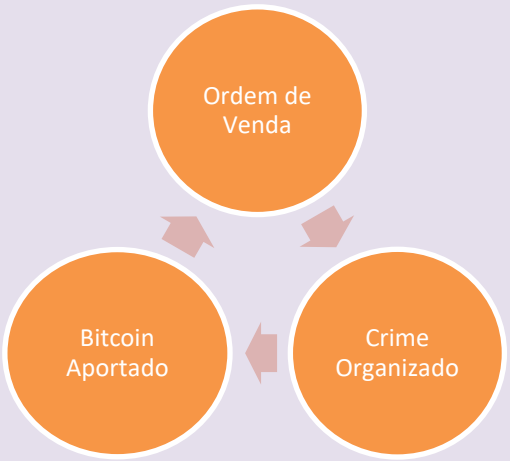
Através da exploração de falhas de implementação de controle de acesso nas aplicações interligadas ao ADFS, o Crime Organizado ganha acesso ao ADFS.

Transferência bancária por meio de resgate (lavagem de dinheiro)

Ativo	Solicitação de Resgate
Mecanismo	Bitcoin Vendido
Atacante	Crime Organizado
Probabilidade	ALTO
Impacto Técnico	NENHUM
Impacto Negócio	MÉDIO
Risco	**ALTO**

Por meio da solicitação do resgate da venda dos bitcoins de origem duvidosa, o Crime Organizado realiza a transação que justificará a origem de seus recursos financeiros, concretizando a lavagem de dinheiro.

Venda de bitcoin aportado



Ativo	Ordem de Venda
Mecanismo	Bitcoin Aportado
Atacante	Crime Organizado
Probabilidade	ALTO
Impacto Técnico	ALTO
Impacto Negócio	MÉDIO
Risco	**CRÍTICO**

Através da colocação de ordens de venda, o Crime Organizado converte de fato seus bitcoins em moeda corrente (R$).

Aporte de bitcoin por verificação burlada

Ativo	Aporte de Bitcoin
Mecanismo	Verificação Burlada
Atacante	Crime Organizado
Probabilidade	ALTO
Impacto Técnico	MÉDIO
Impacto Negócio	BAIXO
Risco	**ALTO**

Com o processo de verificação de origem dos bitcoins burlado, o atacante viabiliza o aporte de bitcoins de absolutamente qualquer origem.

Burla de verificação através de aliciamento

Ativo	Burla de Verificação
Mecanismo	Aliciamento
Atacante	Crime Organizado
Probabilidade	ALTO
Impacto Técnico	BAIXO
Impacto Negócio	BAIXO
Risco	**MÉDIO**

Através do aliciamento dos analistas responsáveis pelo controle de verificação da origem dos bitcoins, o Crime Organizado consegue burlar o processo de verificação de origem dos bitcoins.

Burla de verificação por aporte de carteira limpa

Ativo	Burla de Verificação
Mecanismo	Carteira Limpa
Atacante	Crime Organizado
Probabilidade	ALTO
Impacto Técnico	BAIXO
Impacto Negócio	N/A
Risco	**MÉDIO**

De posse dos dados bancários de clientes com altíssimo poder aquisitivo e muitos recursos financeiros, grupos de crime organizado podem estruturar os sequestros de pessoas VIPs e maximizar seu poder de extorsão em relação ao resgate dessas vítimas de sequestro.

Resgate de bitcoins em carteira limpa

Ativo	Carteira Limpa
Mecanismo	Bitcoins Resgatados
Atacante	Crime Organizado
Probabilidade	ALTO
Impacto Técnico	N/A
Impacto Negócio	BAIXO
Risco	**MÉDIO**

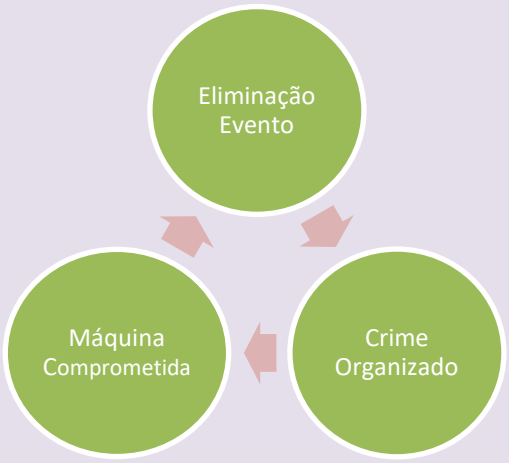
Através do resgate dos bitcoins em uma carteira limpa (virgem), o crime organizado consegue “limpar” seus bitcoins, tornando-os irrastreáveis para o processo do Chainalysis.

Aporte sujo em Exchange sem validação

Ativo	Aporte de Bitcoin Sujo
Mecanismo	Ausência de Validação
Atacante	Crime Organizado
Probabilidade	ALTO
Impacto Técnico	N/A
Impacto Negócio	BAIXO
Risco	**MÉDIO**

O Crime organizado efetua o aporte de seus bitcoins de origem duvidosa em exchanges que não fazem a validação de origem de bitcoins para ludibriar a validação do Chainalysis.

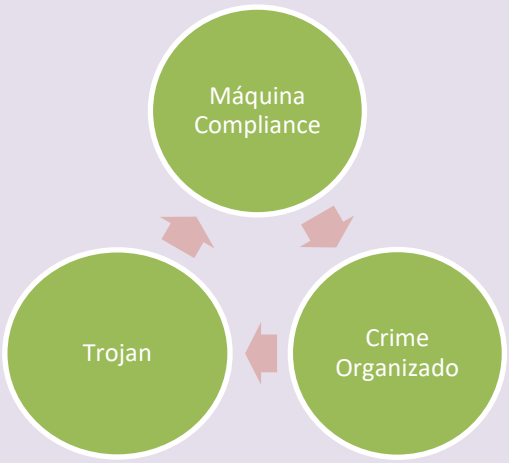
Eliminação de evento de através de máquina comprometida



Ativo	Eliminação Evento
Mecanismo	Máquina Comprometida
Atacante	Crime Organizado
Probabilidade	MÉDIO
Impacto Técnico	BAIXO
Impacto Negócio	BAIXO
Risco	**BAIXO**

Através dos acessos conquistados com a máquina comprometida do analista de compliance o atacante envia comandos diretamente para o BackOffice de compliance “aprovando o aporte” e eliminando o evento da lista de trabalho do analista.

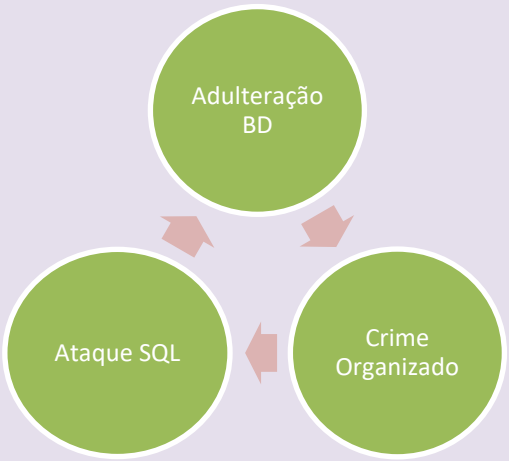
Comprometimento de máquina de compliance por trojan



Ativo	Máquina Compliance
Mecanismo	Trojan
Atacante	Crime Organizado
Probabilidade	MÉDIO
Impacto Técnico	BAIXO
Impacto Negócio	BAIXO
Risco	**BAIXO**

Através do trojan enviado para o analista de compliance, o Crime Organizado ganha acesso à máquina do analista.

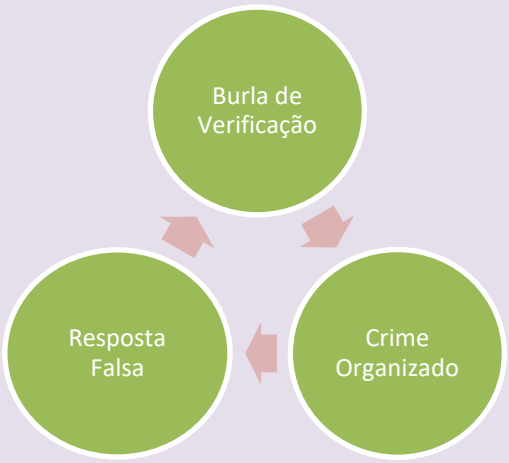
Adulteração de BD por ataque SQL



Ativo	Adulteração BD
Mecanismo	Ataque SQL
Atacante	Crime Organizado
Probabilidade	MÉDIO
Impacto Técnico	BAIXO
Impacto Negócio	BAIXO
Risco	**BAIXO**

Por meio de um ataque SQL em aplicação vulnerável, o Crime Organizado consegue adulterar os registros do banco de dados tornando um aporte bitcoin escuso, legítimo.

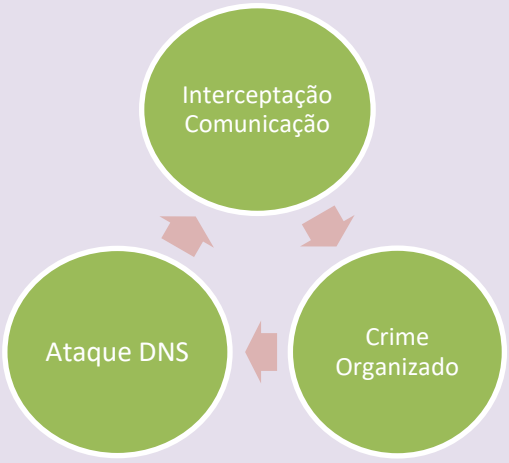
Burla de verificação por resposta falsa



Ativo	Burla de Verificação
Mecanismo	Resposta Falsa
Atacante	Crime Organizado
Probabilidade	MÉDIO
Impacto Técnico	BAIXO
Impacto Negócio	BAIXO
Risco	**BAIXO**

Por meio da adulteração das informações do sistema de verificação (Chainalysis), o Crime Organizado consegue induzir o analista ao erro, fazendo com que ele aprove algo que julga ser legítimo devido a adulteração dos dados.

Interceptação de comunicação do Chainalysis por ataque de DNS



Ativo	Interceptação Comunicação
Mecanismo	Ataque DNS
Atacante	Crime Organizado
Probabilidade	MÉDIO
Impacto Técnico	BAIXO
Impacto Negócio	BAIXO
Risco	**BAIXO**

Por meio de ataque ao DNS, o Crime organizado ludibria a máquina do analista a acreditar estar falando com o servidor legítimo, viabilizando a adulteração da comunicação.

Interceptação de comunicação do Chainalysis por comprometimento do API Manager

Ativo	Interceptação Comunicação
Mecanismo	API Manager
Atacante	Crime Organizado
Probabilidade	MÉDIO
Impacto Técnico	BAIXO
Impacto Negócio	BAIXO
Risco	**BAIXO**

Por meio do API Manager comprometido, o Crime Organizado consegue inserir tratamentos nas chamadas das APIs para adulterar as mensagens e garantir a burla das checagens do Chainalysis.

Hacker: Indivíduo dotado de habilidades técnicas bem desenvolvidas, que permitem a ele invadir ou comprometer sistemas ou subverter regras de negócio – através da exploração de vulnerabilidades – com o objetivo de lucro monetário. Este tipo de atacante também pode agir como um Fraudador quando necessário.

Furto de bitcoins de cliente (via trading)

Ativo	Furto do Cliente
Mecanismo	Trading Fraudulento
Atacante	Hacker
Probabilidade	ALTA
Impacto Técnico	MÉDIO
Impacto Negócio	ALTO
Risco	**CRÍTICO**

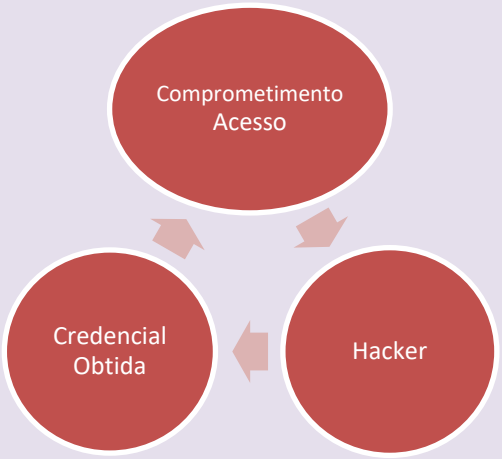
Com o poder de controlar o trading, o Hacker cancela todas as ordens de compra existentes, deixando apenas a sua própria (com valor absurdamente baixo), e adiciona uma ordem de venda para a vítima também com valor absurdamente baixo, forçando que os bitcoins da vítima sejam vendidos para ele.

Manipulação do mecanismo de trading (vulnerabilidade)

Ativo	Fraude no Trading
Mecanismo	Vulnerabilidade
Atacante	Hacker
Probabilidade	ALTA
Impacto Técnico	MÉDIO
Impacto Negócio	MÉDIO
Risco	**ALTO**

O Hacker identifica e explora uma vulnerabilidade no mecanismo de trading (por exemplo, uma escalação de privilégios) que permite a ele adicionar e cancelar ordens de compra e venda arbitrariamente, viabilizando a fraude no mecanismo de trading.

Comprometimento do acesso por obtenção de credenciais (por força bruta ou hacking)

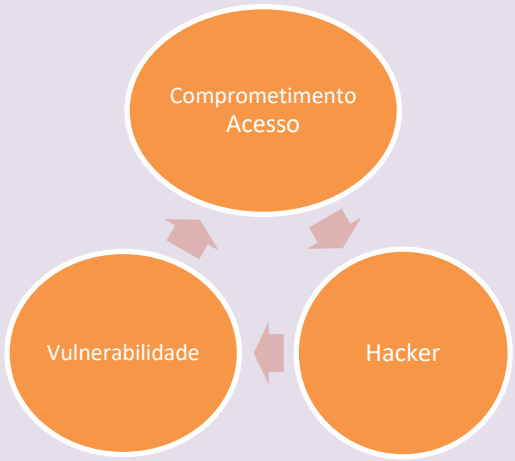


Ativo	Comprometimento Acesso
Mecanismo	Credencial Obtida
Atacante	Hacker
Probabilidade	ALTA
Impacto Técnico	MÉDIO
Impacto Negócio	MÉDIO
Risco	**ALTO**

Em posse da credencial de acesso do usuário, o Hacker obtém “acesso” a sua conta.

Tal credencial pode ser obtida via força bruta, ou através do comprometimento da máquina ou do serviço de email da vítima.

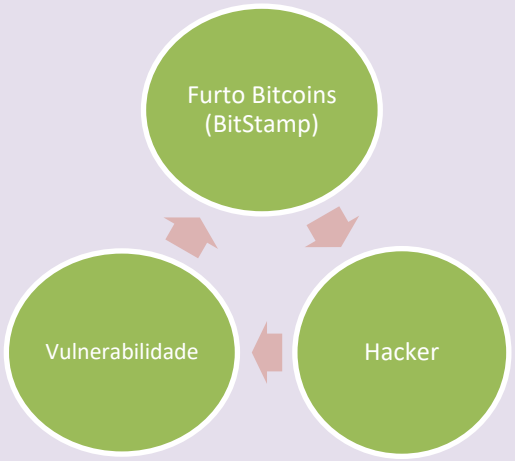
Comprometimento do acesso por vulnerabilidade



Ativo	Comprometimento Acesso
Mecanismo	Vulnerabilidade
Atacante	Hacker
Probabilidade	MÉDIA
Impacto Técnico	MÉDIO
Impacto Negócio	MÉDIO
Risco	**MÉDIO**

Valendo-se de uma vulnerabilidade no frontend acessado pelo cliente, o Hacker é capaz de obter acesso não autorizado à conta do mesmo, ou mesmo fazer o bypass do 2FA solicitado.

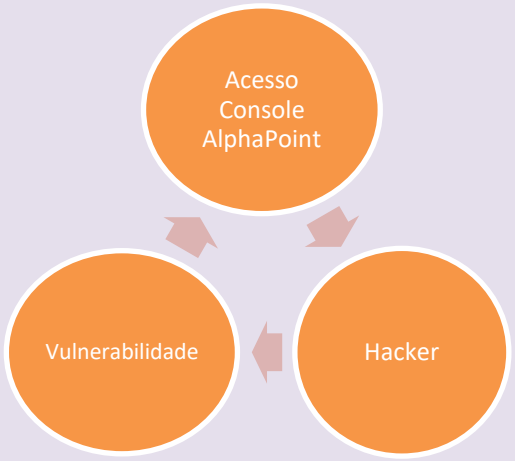
Desvio de bitcoins para outra wallet (vulnerabilidade)



Ativo	Furto Bitcoins (BitStamp)
Mecanismo	Vulnerabilidade
Atacante	Hacker
Probabilidade	BAIXA
Impacto Técnico	BAIXO
Impacto Negócio	BAIXO
Risco	**BAIXO**

Um Hacker que eventualmente identifique e explore vulnerabilidades na BitStamp, pode ser capaz de furtar bitcoins da EXCHANGE que se encontrem na plataforma.

Acesso à console do AlphaPoint por vulnerabilidade

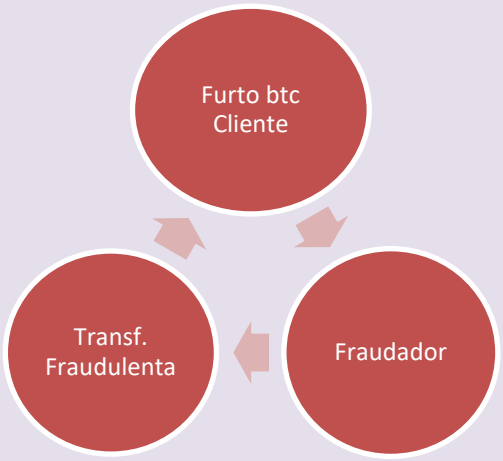


Ativo	Acesso Console AlphaPoint
Mecanismo	Vulnerabilidade
Atacante	Hacker
Probabilidade	BAIXA
Impacto Técnico	MÉDIO
Impacto Negócio	MÉDIO
Risco	**MÉDIO**

Um Hacker que identifique e explore vulnerabilidades na console administrativa do AlphaPoint, ganhará acesso à mesma.

Fraudador: Indivíduo sem habilidades técnicas, mas com uma mente subversiva e capaz de executar golpes com maestria, geralmente fazendo uso de engenharia social. Dentre as técnicas empregadas por este atacante, pode-se destacar: *phishing* (por email, SMS, telefone, etc.), *websites* clonados, SIM *swap*, entre outras.

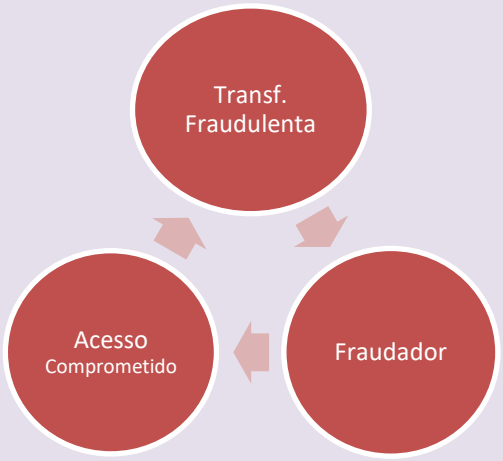
Furto de bitcoins de cliente (via transferência)



Ativo	Furto btc Cliente
Mecanismo	Transferência Fraudulenta
Atacante	Fraudador
Probabilidade	ALTA
Impacto Técnico	BAIXO
Impacto Negócio	MÉDIO
Risco	**ALTO**

O Fraudador, com acesso à conta do cliente, realiza uma transferência fraudulenta dos bitcoins da vítima para uma wallet sob seu controle.

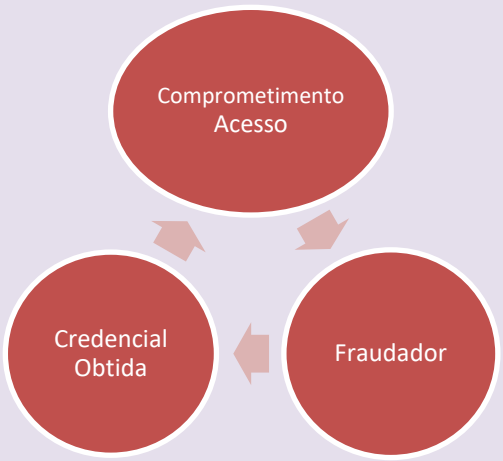
Transferência por meio de acesso comprometido



Ativo	Transferência Fraudulenta
Mecanismo	Acesso Comprometido
Atacante	Fraudador
Probabilidade	ALTA
Impacto Técnico	BAIXO
Impacto Negócio	MÉDIO
Risco	**ALTO**

A partir do acesso comprometido à conta do cliente, o Fraudador realiza uma transferência fraudulenta.

Comprometimento do acesso por obtenção de credenciais (por bases vazadas ou phishing)

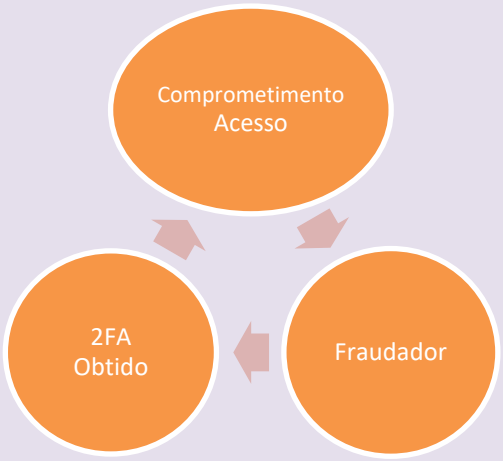


Ativo	Comprometimento Acesso
Mecanismo	Credencial Obtida
Atacante	Fraudador
Probabilidade	ALTA
Impacto Técnico	MÉDIO
Impacto Negócio	MÉDIO
Risco	**ALTO**

Em posse da credencial de acesso do usuário, o Fraudador obtém “acesso” (parcialmente) a sua conta.

A credencial pode ser obtida por meio de bases vazadas, ou via phishing scam.

Comprometimento do acesso por obtenção do 2FA

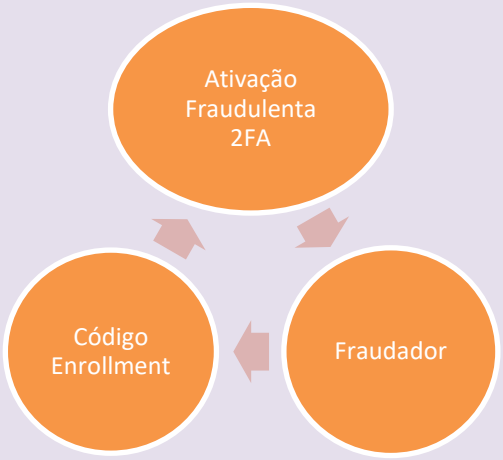


Ativo	Comprometimento Acesso
Mecanismo	2FA Obtido
Atacante	Fraudador
Probabilidade	MÉDIA
Impacto Técnico	MÉDIO
Impacto Negócio	MÉDIO
Risco	**MÉDIO**

Em posse do 2FA do usuário, o Fraudador obtém “acesso” (parcialmente) a sua conta.

O 2FA pode ser obtido por meio do furto do dispositivo do usuário, ou por meio de uma ativação fraudulenta.

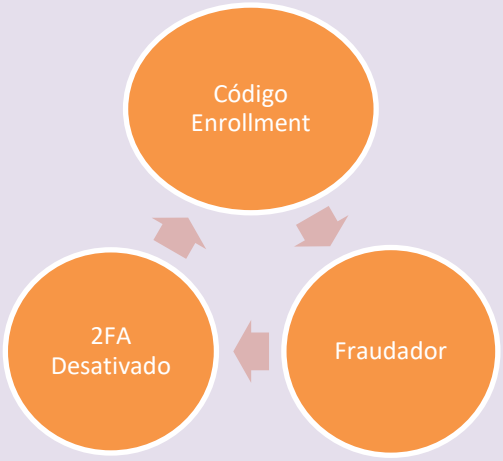
Obtenção do 2FA por ativação fraudulenta



Ativo	Ativação Fraudulenta 2FA
Mecanismo	Código Enrollment
Atacante	Fraudador
Probabilidade	MÉDIA
Impacto Técnico	MÉDIO
Impacto Negócio	MÉDIO
Risco	**MÉDIO**

Uma vez capturado o código de enrollment do usuário (via SIM swap ou phishing), o Fraudador ativa o 2FA do usuário em um dispositivo próprio, a partir de uma função legítima do sistema.

Captura do código de enrollment do usuário



Ativo	Código Enrollment
Mecanismo	2FA Desativado
Atacante	Fraudador
Probabilidade	MÉDIA
Impacto Técnico	MÉDIO
Impacto Negócio	MÉDIO
Risco	**MÉDIO**

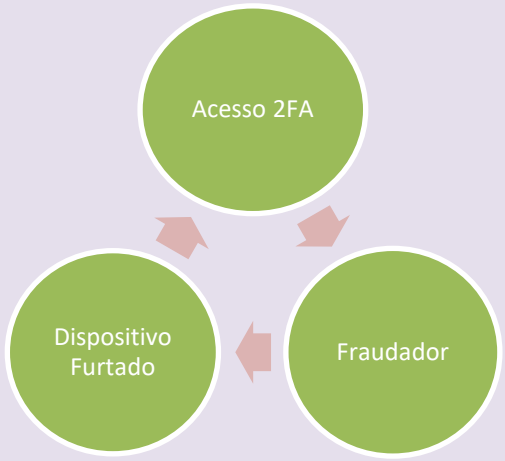
Uma vez que o 2FA do usuário esteja desativado, o Fraudador pode solicitar um código de enrollment a partir de uma função legítima do sistema, e captura-lo via SIM swap ou phishing contra a vítima.

Desativação fraudulenta do 2FA do usuário

Ativo	Desativação 2FA
Mecanismo	Engenharia Social
Atacante	Fraudador
Probabilidade	ALTA
Impacto Técnico	MÉDIO
Impacto Negócio	BAIXO
Risco	**ALTO**

Por meio de engenharia social, o Fraudador é capaz de solicitar que o 2FA do usuário seja desativado, junto ao time de atendimento da EXCHANGE.

Obtenção do 2FA por furto de dispositivo móvel



Ativo	Acesso 2FA
Mecanismo	Dispositivo Furtado
Atacante	Fraudador
Probabilidade	MÉDIA
Impacto Técnico	BAIXO
Impacto Negócio	BAIXO
Risco	**BAIXO**

Uma vez furtado o dispositivo móvel da vítima, o Fraudador acessa os códigos gerados pelo software token (2FA) já associado.