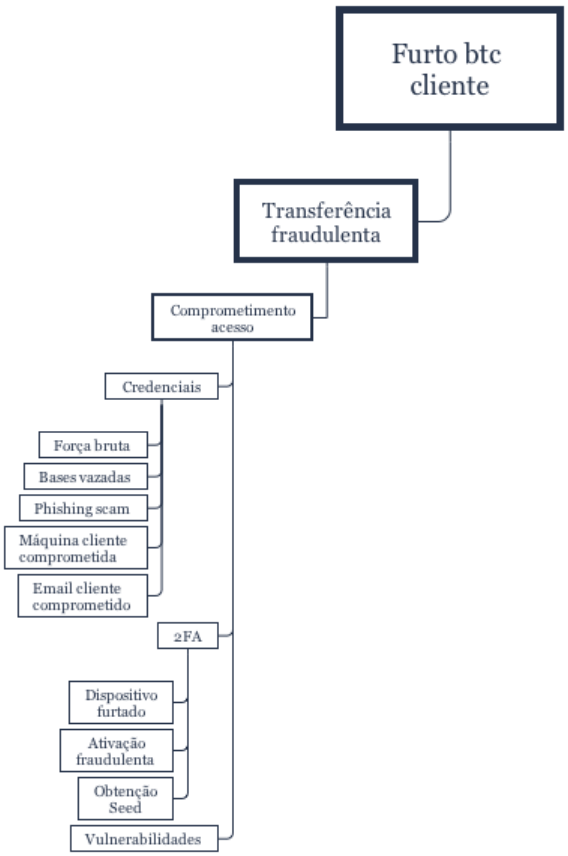
Introdução

Seguem abaixo um conjunto possível de respostas para os exercícios. Não são exaustivas, portanto, você pode ter elucubrado algo diferente e ainda sim correto. Com a prática e a experiência seus modelos serão cada vez mais completos e, portanto, não se desestimule se suas ameaças não se encontrarem aqui. Esse documento visa apenas dar um norte sobre uma das possíveis soluções e deve funcionar mais como balizador do estudo que um simples checklist de acertos e erros. Estude os exemplos e veja se consegue entender na prática a aplicação dos raciocínios explanados nas aulas teóricas.

Ameaças Possíveis

Furto de BTC de clientes

[AME1] Transferência fraudulenta a partir de acesso indevido à conta do cliente



Uma das possíveis formas de furtar BTC da Exchange seria em atacar diretamente os seus clientes.
Um atacante poderia realizar uma **transferência fraudulenta** com objetivo de enviar todos os BTC de um dado cliente para uma *wallet* sob seu controle.
Seria necessário **comprometer o acesso** à conta desse cliente, o que envolveria a **obtenção das credenciais de acesso** (login e senha) do cliente e **do 2FA** do mesmo, ou a **exploração de vulnerabilidades** relacionadas a tais quesitos.

Dentre os mecanismos que viabilizariam o comprometimento do acesso à conta do cliente, pode-se destacar os seguintes:

- Obtenção de credenciais de acesso por meio de **força bruta**, **bases de dados vazadas**, **phishing scam**, ou a partir do **comprometimento do computador** ou **serviço de e-mail** do cliente;

- Obtenção do 2FA a partir do **furto do dispositivo móvel** do cliente, onde o 2FA já se encontra devidamente associado;

- **Ativação fraudulenta do 2FA** do cliente em um dispositivo do atacante, através da obtenção do código de *enrollment* enviado via PUSH Notification. Esse código poderia ser obtido, por exemplo, por meio de engenharia social para capturar o código em questão (e.g. *phishing scam*);

- Obtenção da **seed** (semente) associada ao 2FA do cliente. Essa abordagem consistiria em atacar diretamente o fornecedor do 2FA;

- Exploração de **vulnerabilidades** que possibilitem ao atacante, de alguma forma, obter controle sobre a conta do cliente (e.g. sequestro de sessão ou falhas de controle de acesso); ou ainda falhas que possibilitem a subversão (*bypass*) do mecanismo de 2FA empregado.

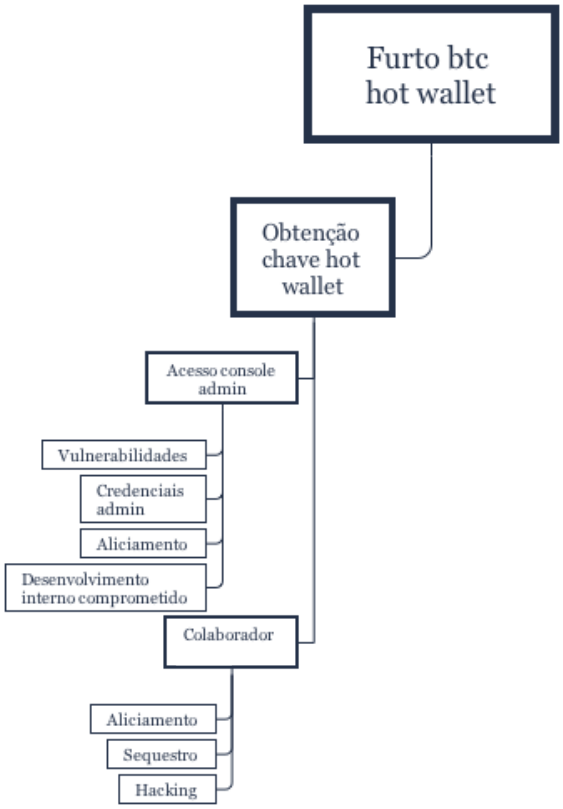
[AME2] Manipulação do mecanismo de trading

Como já mencionado, uma das possíveis formas de furtar BTC da Exchange consiste em atacar diretamente os seus clientes.
Um atacante poderia optar por manipular o mecanismo de *trading*, isto é, **abusar** das funcionalidades que permitem **adicionar ou cancelar ordens de compra e venda**.

Para tal, faz-se necessário a existência de uma vulnerabilidade específica no mecanismo de *trading*, que permitisse ao atacante adicionar e cancelar livremente ordens de compra e venda pertencentes a terceiros. Tal vulnerabilidade caracterizaria uma **escalação horizontal de privilégios**.
Usando esta vulnerabilidade um atacante seria capaz de, por exemplo, cancelar todas as ordens de compra existentes, adicionar uma ordem de compra própria com preço absurdamente baixo e, em seguida, adicionar em nome da vítima uma ordem de venda também com preço absurdamente baixo. Dessa forma, o mecanismo de *trading* não teria outra opção senão vender os BTC da vítima aceitando a única ordem de compra existente, pertencente ao atacante.

Furto de BTC da hot wallet (AlphaPoint)

[AME3] Obtenção da chave privada referente à hot wallet

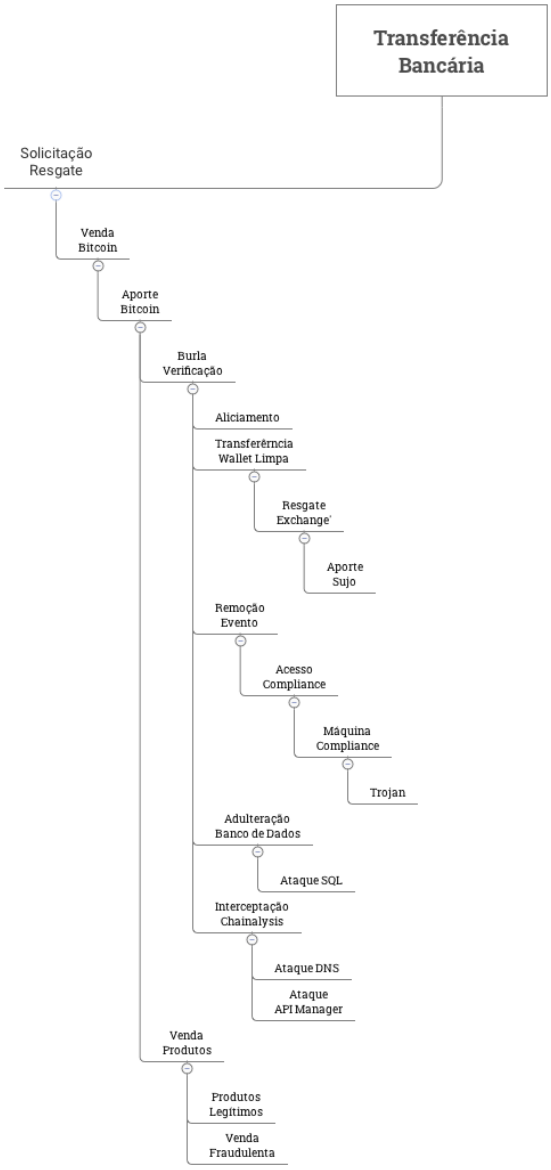


Uma das possíveis formas de furtar BTC da Exchange consiste em atacar diretamente a *hot wallet* localizada no ambiente do AlphaPoint.
O atacante precisaria apenas **obter a chave privada** referente à *hot wallet* e, em seguida, transferir os BTC armazenados para uma *wallet* sob seu controle.
A chave em questão poderia ser obtida a partir do acesso à **console administrativa do AlphaPoint** – através de uma vulnerabilidade ou *backdoor* no sistema, através da obtenção de credenciais de acesso de um usuário com privilégios suficientes, ou por meio de aliciamento.

O objetivo do atacante também poderia ser alcançado a partir um **colaborador da Exchange** que tenha acesso a um *backup* dessa chave. Dentre os meios para isso, pode-se citar: aliciamento, *hacking* de dispositivos relevantes e até mesmo sequestro.

Lavagem de dinheiro

[AME5] Lavagem de dinheiro através de operações de BTC



Para esta ameaça o principal atacante é o Crime Organizado, uma vez que esse perfil de atacante dispõe muitas vezes dos recursos necessários, bem como do interesse em buscar caminhos para efetuar essa ação da lavagem de dinheiro.

Para concretizar a lavagem, basta que o Crime Organizado consiga efetuar o aporte de seus BTC (de fontes duvidosas, ou mesmo de fontes combinadas – usando negócios legítimos para complicar a identificação real da origem do dinheiro) e na sequência consiga efetuar algumas transações simples de venda dos BTC, viabilizando o passo final que consiste na retirada dos fundos (valores em moeda corrente).

O atacante vai utilizar outras *exchanges* que aceitam seus BTC e que, ao transferir seus BTC “de fonte duvidosa” para a *exchange* e retirá-los dias depois para uma *wallet* “limpa” ele consegue fazer o aporte em uma conta da Exchange.

A burla da verificação pode ser atingida por alguns caminhos, dentre eles o mais provável é o caminho mais explorado pelo Crime Organizado, o do aliciamento. O Crime Organizado tem por padrão de operação sempre que possível corromper a fiscalização garantindo não só que ela não ocorra, mas também tornando o agente de fiscalização um aliado que trabalhará ativamente para que o esquema não seja identificado, uma vez que ele será diretamente implicado no esquema. Assim, investigar um cenário com agente de fiscalização corrompido, neste caso um colaborador da área de *compliance*, seria

extremamente complicado porque, em teoria, ele é o último nível da fiscalização.

Nesse ponto, temos os dois caminhos mais prováveis de serem encontrados pelos atacantes dada sua familiaridade com esse tipo de mecanismo de ataque (corrupção e processos simples de operação de *trading*), mas não podemos descartar o carácter "organizado" do atacante que dispõe, em seu arsenal, de pessoal com capacidade técnica avançada e preparado para ataques mais sofisticados do ponto de vista técnico.

Um dos mecanismos técnicos mais amplamente utilizados por eles é o envio de *trojan* por e-mail, ou através de sistemas na web que ele saiba que sua vítima utiliza. Nesse caso ele tem um caminho ideal que é o envio de documentos devidamente adulterados para execução de código malicioso na máquina da equipe de *compliance*. Neste caso, o PDF de imposto de renda que é enviado legitimamente por clientes e aberto com naturalidade pelos analistas. Tudo sem despertar qualquer tipo de suspeita.

O atacante após algumas tentativas vai infectar a máquina de *compliance*, provavelmente passará algum tempo observando o *modus operandi* do analista, e é nesse processo de observação que ele vai identificar o tratamento dado pelo analista às contas barradas. Nesse ponto ele identificará que se trata de um sistema web e tentará executar o ataque da forma mais furtiva possível, que é efetuar a adulteração no sistema através dos mesmos passos e comandos que seriam dados pelo analista, fazendo parecer que o analista analisou e decidiu por "liberar" aquele aporte "de fonte duvidosa".

Ele provavelmente fará isso identificando os comandos dados pela própria interface do *compliance* e cuidadosamente automatizando o disparo de uma sequência de comandos projetada para gerar os devidos *requests* e *logs* que um tratamento manual corriqueiro do analista gerariam. Entretanto ele fará isso apenas para seus aportes em suas contas, e mais, no momento em que o próprio analista estiver logado no sistema para fazê-lo usando a sessão estabelecida pelo analista de *compliance* e sem a necessidade de quebrar a senha ou outros mecanismos de controle de acesso. Feito isso o Crime Organizado terá concretizado a "Remoção do evento" de análise gerado pelo sistema, fazendo com que o analista nem perceba que um dia ele esteve lá.
Se o Crime Organizado não conseguir seguir pelo caminho sorrateiro, ele ainda tem dois mecanismos técnicos, mas que possivelmente chamariam a atenção

de um time de monitoração de segurança (caso exista – e ele não sabe até esse ponto se tal time existe ou não).

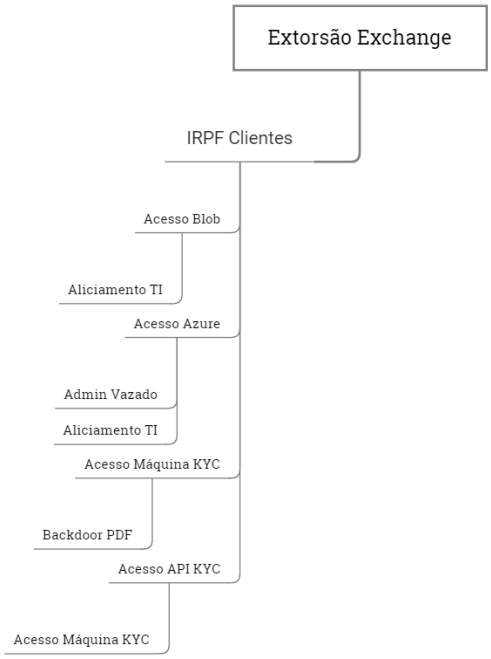
Ele pode optar por atacar o banco de dados diretamente através de tentativas de injeção de SQL em *requests* de qualquer interface de *BackOffice* (cadastro e *compliance* mais provavelmente, mas até a do financeiro poderia ser usada). Com esse acesso direto ao envio de comandos ao banco de dados ele poderia identificar o modelo de dados, as tabelas e como é armazenada a *flag* que determina que um aporte está vindo "de fonte duvidosa", e simplesmente removê-la dando continuidade ao aporte.

Por último, a opção mais sofisticada e cara do ponto de vista do ataque e, portanto, provavelmente a última coisa a ser tentada pelo atacante, seria o ataque ao DNS, fazendo com que o analista de *compliance*, ao consultar o sistema de validação de aportes, na verdade consultasse um *proxy* do atacante com capacidade de entender o que o analista estaria consultando e seletivamente adulterar as respostas do sistema de validação de aportes para que o analista recebesse uma resposta fraudada (uma vez que a resposta à consulta para a *wallet* do atacante estaria sendo filtrada pelo *proxy*). Essa resposta sinalizaria sempre que as *wallets* do atacante seriam legítimas e fariam o analista tomar a decisão errada.

Como toda a infraestrutura de *backend* e mensageria de serviços está apoiada em um API *Manager*, ou seja, todas as requisições de serviço de *backend* passam por esse ponto único de controle de acesso, seria plausível que o atacante tentasse atacar o API *Manager* através de vulnerabilidades na própria camada de serviço da Microsoft, ou mesmo conseguindo acesso à interface e plantando regras de roteamento para que o API *Manager* direcionasse o tráfego de validação para um *proxy* de controle do atacante que realizaria a mesma lógica de adulteração das mensagens.

Extorsão contra a Exchange

[AME6] Extorsão mediante vazamento de dados (IRPF)



Para um atacante, é trivial descobrir que a Exchange solicita o envio do IRPF para aprovação do cadastro de um usuário. Isto porque muitos Fraudadores e o próprio Crime Organizado criarão contas na plataforma da Exchange. Isso pode chamar a atenção desses dois perfis de atacantes para o cenário da extorsão mediante vazamento de dados sigilosos, neste caso, do IRPF dos clientes legítimos.

Um dos caminhos iniciais mais prováveis seria o caminho do atendimento. Uma vez que o time de atendimento reporta cenários de solicitações de clientes que demandem análise do time de cadastro (KYC) ou do time de *compliance*, que anexam no sistema o IRPF quando cabível, eles têm acesso direto ao documento.

Sendo o atacante o Crime Organizado, o mecanismo mais provável seria o do aliciamento. O Crime Organizado tem por padrão de operação sempre que possível corromper agentes legítimos do processo garantindo não só seu ataque, mas também tornando o agente um aliado que trabalhará ativamente para que o esquema não seja identificado, uma vez que ele será diretamente implicado no esquema.

Se o aliciamento falhar, ainda há a possibilidade de ataques mais técnicos como o do envio de *trojan* por email, ou através de sistemas na web que ele saiba que sua vítima utiliza. Nesse caso ele tem um caminho ideal que é o envio de documentos devidamente adulterados para execução de código malicioso na máquina da equipe de atendimento, que é o PDF de imposto de renda enviado legitimamente pelos clientes e aberto com naturalidade pelos analistas. Tudo sem despertar qualquer suspeita.

Por fim, é possível, dado que se trata de um sistema web e que a operação de atendimento tende a ter muitas trocas de pessoal e com isso uma certa

reutilização de acessos a ferramenta Web, que o atacante tente simplesmente um ataque de força bruta para identificar as senhas dos atendentes.

> NOTA
>
> Presume-se para essa análise que há certo *turnover* no time de atendimento e que não há contas nominais para todos os analistas de atendimento e, portanto, que não há como habilitar um segundo fator de autenticação (2FA) para essas contas.

Um dos mecanismos técnicos utilizados seria o envio de *trojan* por e-mail, ou através de sistemas na web que ele saiba que sua vítima utiliza. Nesse caso ele tem um caminho ideal que é o envio de documentos devidamente adulterados para execução de código malicioso na máquina da equipe de cadastro (KYC).

Neste caso, o PDF de imposto de renda que é enviado legitimamente pelos clientes e aberto com naturalidade pelos analistas. Tudo sem despertar qualquer tipo de suspeita. Com isso o atacante teria então acesso às máquinas do time de cadastro e tudo mais contido nelas, inclusive os PDFs que foram abertos por eles (em *cache*, ou salvos localmente). Uma vez que as APIs de *backend* de cadastro são acessadas diretamente desta máquina, basta que o atacante consiga mapear o *request* de consulta de clientes e replicá-lo através da máquina da equipe de cadastro para percorrer toda a base de dados de clientes e seus devidos documentos armazenados. No caso, os PDFs dos impostos de renda.

Um terceiro caminho para o atacante seria ir direto a TI, através de buscas em redes sociais como Facebook e LinkedIn, identificar os analistas de TI que trabalham para Exchange e abordá-los com o aliciamento para obter acesso direto ao ponto de armazenamento dos documentos: o *Blob*. Isso pode ser viável com certo baixo investimento no caso de colaboradores com acesso que sejam desligados do time, mas que tenham seus acessos mantidos por dias ou semanas além do seu desligamento, ou mesmo para colaboradores descontentes que vejam a oportunidade de lucro rápido.
Isto porque enquanto não houver o controle de 2FA generalizado para o *staff* e acessos de TI, sempre haverá o álibi de sua conta ter sido invadida, ou mesmo, de que sua senha tenha sido quebrada, inviabilizando a punição direta, mesmo que o acesso seja auditável. Esse ataque pode ser mais danoso ainda se for endereçado aos analistas com acesso à conta Admin do Azure. Essa conta “root” tem um papel amplo na configuração do ambiente e dará acessos muito privilegiados ao atacante, inclusive permitindo que ele apague seus rastros após o ataque.

Esse acesso pode ser comprometido tanto por aliciamento quanto por um vazamento simples, ou seja, descuido ou imprudência dos analistas de TI durante sua operação do dia-a-dia. O uso de senhas fáceis ou comuns, ou mesmo a ausência de um segundo fator de autenticação (2FA) podem expô-lo.