# Como pensar na área de Segurança em Computação

Vinicius Macelai

Agosto 2019

## 1 Sistema escolhido

O sistema escolhido foi o do *Bitcoin*[1]. Por mais que não seja um sistema que utilizo corriqueiramente, acredito que seja sistema relevante para a disciplina de Segurança em Computação.

## 2 Ativos

Ao pensar em um ataque ao Bitcoin podemos pensar em diversos ativos que podemos atacar. Pode-se atacar diretamente a rede, no caso sua *blockchain*, ou atacar os seus usuários.

### 2.1 *Blockchain*

Ao atacar a *blockchain* do *Bitcoin*, o seu maior ativo direto são as criptomoedas em circulação, assim o atacante pode realizar um ataque de gasto duplo, utilizando de grande poder computacional para enganar a rede e conseguir realizar transações fraudulentas e enganando usuários, causando prejuízo financeiro para tais.

Indiretamente há o ativo da confiança no sistema, pois qualquer ataque bem sucedido a sua *Blockchain*, há a perda de confiança no sistema, podendo causar uma séria desvalorização do preço da criptomoeda. Que pode ter como consequência o fim do projeto.

### 2.2 Usuários

Ao atacar usuários que utilizam do *Bitcoin*, o ataque pode ser diretamente ao usuário ou a sistemas de terceiros que o usuário participa, como *exchanges*. O pior ataque ao usuário seria invandir a carteira que detêm a posse das criptomoedas e roubar seu saldo, isso pode ser feito tanto na carteira individual do usuário, tanto na carteira coletiva da *exchange*. Caso o ataque for na *exchange*,

pode levar a falência da empresa, caso seja um ataque a uma carteira com muito valor da empresa.

Um outro ataque indireto seria o de obter informações sobre o detentor de uma determinada carteira, como no *Bitcoin* as carteiras são um pseudônimo do usuário real, ao descobrir o real dono de uma carteira, você teria informações sensíveis como o que ele compra com suas criptomoedas, além de poder determinar um perfil da pessoa

# 3 Adversários

## 3.1 Hacker visando benefício finaneiro

Há diversos casos onde uma pessoa com interesse de obter vantagem financeira pode atacar tanto um usuário individual, quanto as *exchanges*. Não acredito que um ataque a *blockchain*, visando um gasto duplo, tenha interesse financeiro, visto que tal ataque iria acabar com reputação da moeda, causando prejuízo financeiro num modo geral, consequentemente o gasto duplo que ele fez seria mínimo com o custo do ataque.

## 3.2 Governos

Pensando de forma mais conspiracionista, os Governos tem interesse em atacar uma rede como a do *Bitcoin*, visto que essa tecnologia permite a descentralização do dinheiro, onde na atualiadade isso é mantido pelos bancos centrais dos Governos, que têm seus próprios interesses para se manterem relevantes, pois há um grande poder em mandar na forma do dinheiro.

# 4 Gerenciamento de risco

O que uma invasão pode custar? Basicamente se for um usuário leigo que guarda todo o seu saldo em uma única carteira, pode custar todo o seu dinheiro guardado, causando um enorme prejuízo. Se for um ataque visando buscar informações sobre as movimentações da pessoa, pode-se obter informações sensíveis que podem ser utilizadas em outro tipo de ataque direto a pessoa.

As probabilidades de acontecer um ataque contra um usuário são altas, visto que um único ataque pode acarretar em prejuízos milionários e há diversos relatos de usuários que não seguem boas práticas, sendo alvos fáceis.

# 5 Contra medidas

- Uso de carteiras em hardware, visto que elas provem uma maior segurança de modo geral.
- Boas práticas de privacidade, como usar apenas uma vez um endereço.

- Utilização de algoritmos bem estudados e seguros na *blockchain*.
- Não utilizar *exchange* como carteira.

A maior contra medida não técnica que está presente no *Bitcoin* é a questão do incentivo, o projeto inteiro foi criado pensando na teoria dos jogos, onde o incentivo para continuar seguindo as regras do jogo é muito grande, visto que um ataque de gasto duplo gastaria muito dinheiro e esse dinheiro seria melhor aplicado caso apenas seguisse as regras do jogo.

# 6 Custo/Benefício

Ao mirar um ataque a *blockchain*, é observado um custo/beneficio praticamente zero, visto que o custo para ter processamento computacional seria em torno de bilhões de dólares para um único ataque, dificilmente esse único ataque iria valer a pena o gasto total, consequentemente esse ataque diminuiria o valor da moeda devido a quebra de confiança dos participantes do sistema, fazendo com que próximos ataques sejam menos atrativos ainda.

Ao tentar atacar um usuário da rede, depenendo do tipo de ataque, normalmente não há custo, tendo em vista que os ataques acontecem devido a descuidos do usuário ou de utilizam de ferramentas de terceiros que detêm falhas comuns, ou até mesmo o uso de engenharia social para obter vantagens, um único ataque bem sucedido pode ter belo retorno para o adversário.

# References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009.