Common Targeted Attacks

Within the world or cryptocurrency and the threats that come with it, there is a plethora of attacks on people’s property and assets gained through cryptocurrencies. And while all of these attacks are should be taken seriously in their own respect, there are a few of these attacks that are more common than others and should be addressed first. Starting things off we have Attacks on Wallet Software. There are client style applications that are known as wallets and just like a physical wallet, it is used to store and manage Bitcoin and other cryptocurrencies. The client would be able to either have a virtual or online wallet option, or the user can download that software to his or her node. Online wallets are more susceptible to attacks and for that reason there should be some type of offline backup encryption of said wallet. Distributed denials of service (DDoS) attacks are also some of the most formidable forms of this type of attack.

Next, we have timejacking attacks. This includes how the attacker would give out the incorrect time logging information when connecting to a node for a transaction. This way, the network and the counter of the node is changed and altered by the attacker and the node that has been affected by this has the potential to falsely accept an alternate blockchain than the one that was already in use. Reasons why this attack is one of the most dangerous attacks is because of the consequences that can arise because of it. Double-spending which is another type of attack is something that can result from it and become an even bigger problem than it already was, and the resources it would take during the mining process would essentially have been wasted which costs a lot of money and valuable time.

The ‘>50%’ Attack is a major threat for in the cryptocurrency realm of things. This targets the mining process, and is when there is a user of some sort obtaining over 50% of all computing resources needed for the mining to begin. Once a user or users have access to this type of power and control, they can exclude, modify, self-reverse transactions, and even potentially prevent mining of blocks for their own personal benefit. Yet, it has been noted by researchers that even if the hackers have just around 40% of the computing resources, the attackers can still prove to be a formidable threat and have a 50% chance of success with their attack. To help reduce these types of attacks, is to establish a set in stone checkpoints so then if there are blocks before the checkpoint, they cannot be altered. Yet, if this attack in particular is successful, then the attacker(s) can do some serious damage to the whole system. A study conducted at Cornell University shows us that a ‘>50%’ attack is very possible to happen because in a network in a single mining pool only control around 25%-33% of the overall mining power.

Double spending is also something that is a very serious threat for cryptocurrency transactions. This is when the attacker is able to make more than one transaction by using the same “coin” for multiple transactions; invalidating what an honest transaction should be. The most common way this attack would happen would be in a way of a quick payment mode. The attacker would be able take a specific coin and make a transaction at the same time that another transaction has been made using that same coin with a different address than the first one. By doing this and altering the timestamp, the illegal and false transaction can be made to be a real one. And through this type of attack, the original receiver would not be able to authenticate the transaction to confirm its truthfulness. Because of this type of attack ‘observers’ have been placed in the network to monitor this type of activity.

Lastly, to round out this list of harmful attacks, we have selfish mining. This deals with having a group of miners that spend their time and resources with respect to computing power to mine cryptocurrencies and then those uncovered blocks will not be added to the blockchain which would cause time and resources by other miners to be used wastefully but unknowingly. The group of miners who are forcing the honest miners to do this, will keep the blocks that they mined private to perform some type of divergence to the blockchain, while coincidingly keeping the honest miners using their resources to waste them. Essentially the greedy miner will work diligently to nullify the honest and truthful miners hard work.