Eclipse Attacks on Monero's Peer-to-Peer Network (Attacking the Mainnet)

Anonymous Authors

September 12, 2024

Abstract

This document serves as a supplement to our NDSS 2025 submission "Eclipse Attacks on Monero's Peer-to-Peer Network". We experimented with our proposed Eclipse attack on Monero's Mainnet. Compared to the testnet experiments, our attack on the mainnet consists larger network size (approx. **2000**+) and node records (**1000** in whitelist & **5000** in graylist).

Experimental results show that our attack can effectively occupy **ALL** connections of Monero nodes under the mainnet environment at a negligible cost (**0.06 USD**).

1 Experiment Preparation

1.1 An Overview of Monero mainnet

The Monero mainnet, launched in April 2014, is the production network of Monero. It has undergone several major updates (https://github.com/monero-project/monero?tab=readme-ov-file#scheduled-softwarenetwork-upgrades). The node version we utilized for our experiments is v0.18.3.1 (refer to https://github.com/monero-project/monero/releases/tag/v0.18.3.1). Our attacks were conducted on the current live version of the mainnet.

1.2 Configurations

Network size. According to our latest Monero network probe results, during the supplementary experiments, the Monero main network contains approximately **2,200** active nodes, which is much larger than our test network where the number of active nodes ranges from 20 to 30.

Hardware/software settings. Similar to the experimental setup of the testnet, we also run Monero nodes on two servers (Server A & B) with public IP. Server A runs modified Monero node as our target node. Server B runs 1000 simulated Monero nodes as the attacker's malicious node resources. In addition, we also run 20 nodes behind NAT for the graylist attack.

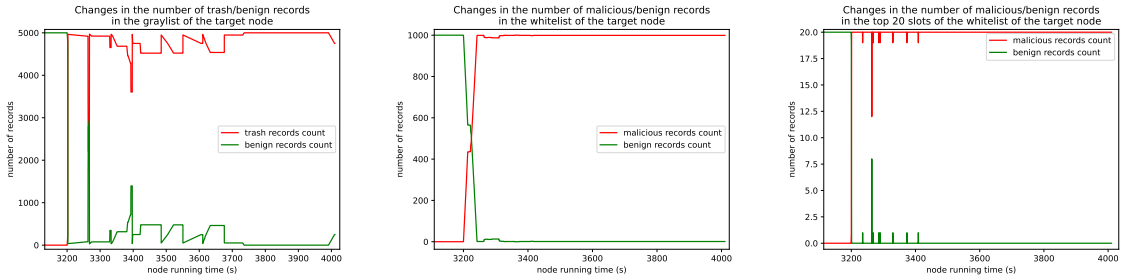
Both servers have the same physical configuration, which includes an Intel(R) Xeon(R) Platinum 8255C CPU @ 2.50GHz 4C4T, 8GB of memory, a network bandwidth of 12Mbps, and running Ubuntu Server 20.04 LTS 64-bit.

1.3 Target Node Info

For ethical reasons, we deployed a full node with a public IP in the mainnet as the target node for the experiment. Before the attack, the basic situation of the node is as follows:

Graylist & Whitelist. The number of benign node records in the target node graylist and whitelist are **5,000** and **1,000**, respectively. It can be seen that as the network size increases, the number of benign node records in the node graylist/whitelist also increases significantly. In contrast, in our TestNet experiments, the number of benign node records in the node graylist and whitelist are only about 1500 and 30, respectively.

Connections. We allowed the node to run in the network for approximately 2 hours to ensure its connection status reached a stable state. The target node maintained 12 outgoing connections, while the number of incoming connections fluctuated between 25 and 35.



(a) Node records in the graylist attack

(b) Node records in the whitelist attack

(c) Top-20 node records in the whitelist attack

Figure 1: Evaluation on the graylist/whitelist attack

2 Launching Attack

To ensure the attack closely mirrors real-world conditions, we did not attempt to gather any status information about the target node during the entire attack process. Instead, we relied solely on the information that would be available to an attacker to assess the success of the attack.

Under this premise, our attack process is as follows:

1. Start 20 malicious nodes to establish incoming connections with the target node and perform graylist attack to pre-fill the graylist of the target node.
2. Perform whitelist attack to fill the target node's whitelist.
3. After the whitelist attack is completed, perform connection reset attack to try to occupy the outgoing connections of the target node.
4. Continue to perform connection reset attack to occupy incoming connections to the target node.
5. Continuously send fluff transactions to the network (these transactions will not be forwarded by malicious nodes to the target node) and detect whether these transactions can be forwarded by the target node to the malicious nodes connected to it. If so, the attacker has not yet achieved complete control of the target node connections, and repeat the attack process. Otherwise, the attack is successful.

3 Experiment Results

We conducted a complete eclipse attack on the target node of the mainnet. Our attack lasted for 13 minutes and 30 seconds and occupied **ALL** the connections of the target node.

We, as follows, analyze the attack results by examining the changes in the content of the graylist and whitelist, as well as the fluctuations in node connections throughout the attack.

3.1 Graylist Attack

In the process of occupying all the connections of the node, the content changes of the target node graylist are shown in Figure 1a. With the launch of the graylist attack, the target node's graylist is quickly occupied by the trash node records, and the number of benign nodes decreases rapidly. However, affected by the target node's timing synchronization mechanism, the number of benign nodes also shows a periodic upward trend, but will soon be overwhelmed by new trash node records. As the target node's benign connections are gradually occupied, the number of benign node records that the target node can obtain gradually decreases. Finally, the trash node records achieve complete occupation of the target node's graylist.

- **Average occupancy rate** is 92.5%. When there is interference from benign connections, it is difficult for the attacker to completely occupy the graylist.

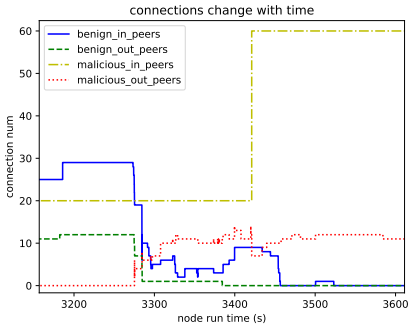


Figure 2: Evaluation on occupying node's connections

- **Effect on selecting out peers** is one of the important indicators for evaluating the graylist attack. During this attack, the node tried to select out peers from the graylist 20 times in total, and only 1 time selected a benign node in the graylist.
- **Effect on *gray_peerlist_housekeeping*** is another important indicators for evaluating the graylist attack. During the attack, the *gray_peerlist_housekeeping* mechanism tried to select record from the graylist 10 times in total and none of them succeeded.

3.2 Whitelist Attack

In the process of occupying all the connections of the node, the content changes of the target node whitelist are shown in Figure 1b and Figure 1c. As the whitelist attack was launched, the number of benign nodes in the target node's whitelist dropped rapidly. Subsequently, due to the target node executing the timed sync mechanism and receiving new incoming connections, the number of benign connections in the target node's whitelist increased slightly.

- **Average occupancy rate** is 97.2%. Affected by the timed sync mechanism and benign connections, it is also difficult to achieve complete occupation of the whitelist. The average occupancy rate for the top 20 slots in the whitelist also reached 99.9%.
- **The impact of benign connections:** During the entire attack, the target node received a total of 30 incoming connection requests from different benign nodes. Although there was interference caused by benign connections in the process, the negative impact on the whitelist attack was relatively small (only 2.8%).

3.3 Occupy Node's Connections

The process of changes in the target node's connections throughout the eclipse attack is illustrated in Figure 2. After initiating both the graylist and whitelist attacks, we executed a total of six connection reset attacks. Over the course of the first five reset attacks, we progressively gained control of all outgoing connections of the target node. The final reset attack successfully expelled all benign incoming connections from the target node.

The entire process, from the initiation of the graylist attack to the takeover of all benign connections, took approximately 13 minutes and 30 seconds, involving six connection reset attacks. In terms of cost, the attack only required around **0.06 USD** (0.01 USD per reset attack, for a total of six resets).

4 Planned Actions

We intend to integrate these results, accompanied by more detailed discussions to align them with the existing experimental findings, into the core of our submitted manuscript. These will be appended following the "Testnet Evaluation" part in Section IV.