Nama : Hanan Mustika Abdurra'uf

NIM : 1103194149

Eclipse Attack

- Jumlah serangan yang dapat dilakukan terhadap jaringan blockchain sangat banyak, dan di antaranya adalah Eclipse Attack. Ini adalah jenis serangan cyber yang bertujuan untuk mengisolasi dan menyerang pengguna tertentu yang merupakan bagian dari jaringan. Semua agar dapat memanipulasi data yang diterima target dari jaringan. Dengan demikian, setiap tindakan jahat dapat dilakukan terhadap korban.

- Jenis ancaman ini dimungkinkan karena struktur dan keterbatasan protokol komunikasi peer-to-peer yang digunakan blockchain. Secara khusus, ini disebabkan oleh pembatasan jumlah koneksi dan pemilihan node yang aman. Misalnya, dalam jaringan Bitcoin, batas koneksi keluar (yang dapat Anda buat dengan node jarak jauh lainnya) adalah 8 koneksi. Ini berarti bahwa setiap node Bitcoin mampu mendukung koneksi dua arah ke 8 node pada saat yang bersamaan. Loop berulang pada setiap node, karena perilaku ini adalah bagian dari protokol yang dijelaskan dalam Bitcoin Core.

- Eclipse Attack juga merupakan sumber dari jenis ancaman yang lebih berbahaya dan luas - Serangan Erebus. Serangan ini mampu melakukan pemadaman skala besar pada jaringan, yang akan menyebabkannya terpecah. Akibatnya, siapa pun yang melakukan serangan Erebus dapat membagi jaringan dan mengelolanya sesuai keinginan mereka, dengan kemampuan untuk melakukan serangan denial of service (DoS), serangan 51%, atau membuat hard fork blockchain.

- Stubborn Mining
  Pada bagian ini, kami memperkenalkan kelas baru Bitcoin
  strategi penambangan, yang disebut penambangan keras kepala, yang secara ketat menghapus (dan memperbaiki) penambangan egois yang diketahui sebelumnya

  Singkatnya, semua penambangan menyimpang yang diketahui strategies bekerja dengan secara selektif menahan blok yang ditambang oleh Di sini kita

membuat asumsi penyederhanaan bahwa jika i j, maka penyerang selalu kalah dalam perlombaan antara penambang publik i to j. Pada kenyataannya, jalur overlay memiliki varians dalam waktu propagasi dan bandwidth, oleh karena itu keberadaan tepi tidak biner, tetapi bisa fraksional. Namun, kami Model dasar cukup untuk memperkirakan rentang γ yang masuk akal.