A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network

Title	A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network
Publication Type	Conference Paper
Year of Publication	2020
Authors	Tran, M., Choi, I., Moon, G. J., Vu, A. V., Kang, M. S.
Conference Name	2020 IEEE Symposium on Security and Privacy (SP)
Date Published	May 2020
Publisher	IEEE
ISBN Number	978-1-7281-3497-0
Keywords	abundant network address resources, ASes, attack execution period, attack traffic rate, bitcoin, Bitcoin core, Bitcoin network, Bitcoin peer-to-peer network, centralization problem, computer network security, eclipse attack, EREBUS attack, Human Behavior, IP networks, Monitoring, natural man-in-the-middle network, network adversary, network operation, peer connections, Peer-to-peer computing, peering decision, peering dynamics, prefix hijacking attack, propagation delays, pubcrawl, public Bitcoin, reliability, Routing protocols, routing-level attacks, Scalability, security, sophisticated attack strategies, stealthier partitioning attack, targeted Bitcoin node, telecommunication network routing, telecommunication network topology, telecommunication traffic, time 5.0 week to 6.0 week

Abstract	Network adversaries, such as malicious transit autonomous systems (ASes), have been shown to be capable of partitioning the Bitcoin's peer-to-peer network via routing-level attacks; e.g., a network adversary exploits a BGP vulnerability and performs a prefix hijacking attack (viz. Apostolaki et al. [3]). Due to the nature of BGP operation, such a hijacking is globally observable and thus enables immediate detection of the attack and the identification of the perpetrator. In this paper, we present a stealthier attack, which we call the EREBUS attack, that partitions the Bitcoin network without any routing manipulations, which makes the attack undetectable to control-plane and even to data-plane detectors. The novel aspect of EREBUS is that it makes the adversary AS a natural man-in-the-middle network of all the peer connections of one or more targeted Bitcoin nodes by patiently influencing the targeted nodes' peering decision. We show that affecting the peering decision of a Bitcoin node, which is believed to be infeasible after a series of bug patches against the earlier Eclipse attack [29], is possible for the network adversary that can use abundant network address resources (e.g., spoofing millions of IP addresses in many other ASes) reliably for an extended period of time at a negligible cost. The EREBUS attack is readily available for large ASes, such as Tier-1 and large Tier-2 ASes, against the vast majority of 10K public Bitcoin nodes with only about 520 bit/s of attack traffic rate per targeted Bitcoin node and a modest (e.g., 5-6 weeks) attack execution period. The EREBUS attack can be mounted by nation-state adversaries who would be willing to execute sophisticated attack strategies patiently to compromise cryptocurrencies (e.g., control the consensus, take down a cryptocurrency, censor transactions). As the attack exploits the topological advantage of being a network adversary but not the specific vulnerabilities of Bitcoin core, no quick patches seem to be available. We discuss that some naive solutions (e.g., whitelisting, rate-limiting) are ineffective and third-party proxy solutions may worsen the Bitcoin's centralization problem. We provide some suggested modifications to the Bitcoin core and show that they effectively make the EREBUS attack significantly harder; yet, their non-trivial changes to the Bitcoin's network operation (e.g., peering dynamics, propagation delays) should be examined thoroughly before their wide deployment.
URL	https://ieeexplore.ieee.org/document/9152616
DOI	10.1109/SP40000.2020.00027
Citation Key	tran_stealthier_2020

abundant network address resources ASes attack execution period attack traffic rate bitcoin Bitcoin core Bitcoin network Bitcoin peer-to-peer network centralization problem computer network security eclipse attack EREBUS attack Human behavior IP networks Monitoring natural man-in-the-middle network network adversary network operation peer connections Peer-to-peer computing peering decision peering dynamics prefix hijacking attack propagation delays pubcrawl public Bitcoin Reliability Routing protocols

routing-level attacks Scalability security sophisticated attack strategies stealthier partitioning attack targeted Bitcoin node telecommunication network routing telecommunication network topology telecommunication traffic time 5.0 week to 6.0 week