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

Muoi Tran, Inho Choi, Gi Jun Moon, Anh V. Vu, Min Suk Kang
May 2020
Bitcoin relies on underlying peer-to-peer network

Bitcoin consensus rules

Peer-to-peer network
Bitcoin peer-to-peer network can be partitioned

**Partitioning attacks:** isolate victim node(s) from the rest of network
Partitioning attack is a **dangerous** threat

Example: *Double spending* attack

Partitioning *enables/improves* several other attacks:
- 51% attack
- selfish mining
- censoring transactions
- take down cryptocurrencies
- ...

---

[Diagram showing partitioning attack and its effects on the Bitcoin network.]
Previous attack: *routing manipulation* to partition Bitcoin’s peer-to-peer network

**All traffic** to victim is *routed* through the attacker!

Victim node

1.2.3.4

Attacker AS

Autonomous System (AS)

**Lie:** “I am the owner of 1.2.3.4”

<table>
<thead>
<tr>
<th>HOME</th>
<th>BLOG</th>
<th>ABOUT US</th>
<th>PRODUCTS</th>
</tr>
</thead>
</table>

**The Canadian Bitcoin Hijack**

*Posted by Andree Toonk - August 12, 2014 - Hijack - N*

A few days ago researchers at Dell SecureW

hijacking BGP prefixes for numerous large

Only **one** attack instance observed in practice. Why?

- Route manipulation is **immediately visible** to the public
- Attacker’s **identity** (AS number) is **revealed**
Can partitioning attacks be **stealthier**?
**Erebus** attack: A **stealthier** partitioning attack against Bitcoin network

**Challenge 2:**
How to influence the target node’s peer selection?

**Idea:** Indirectly force the victim node connects to “shadow” IPs:
- **Shadow IP** has the victim-to-itself route includes adversary AS
- Attacker AS is the **man-in-the-middle** of all peer connections!

**Challenge 1:**
Is there enough shadow IPs that the attacker can use?
**Challenge 1**: How many shadow IPs are available?

If attacker AS is big enough (e.g., top-100), it can *easily* find hundreds of shadow ASes => millions of shadow IPs
**Challenge 2**: How does Erebus attacker influence Bitcoin node’s peer selection?

- Occupying 117 incoming connections *(easier)*
  - Connect to the victim *on behalf* of the shadow IPs

- Occupying 8 outgoing connections* *(much harder!)*
  - Influence the victim to make connections to shadow IPs

(*) 10 outgoing connections since Bitcoin version 0.19.1
How to **influence** the victim to connect to shadow IPs?

**Randomly** choose a **reachable** IP from either of two tables

Victim

Our goal: Dominate **reachable** IPs in two tables with shadow IPs

**Challenges:**
- Several bugs fixed since Bitcoin v0.10.1 (2015)
- Attack is now **nearly impossible** with botnets

In the old days...

Eclipse attack
(Heilman et al., USENIX Sec‘15)
Attack strategy: send *low-rate* traffic and *patiently* wait

Delete *unreachable* IP older than **30 days**

Low-rate traffic

Delete unreachable IP older than **30 days**

1 IP / 2 mins

Most are shadow IPs after **30 days**

Gradually increases

Reachable IPs in the **new** table

Reachable IPs in the **tried** table
Adversary can occupy all connections with shadow IPs in 5 - 6 weeks

All eight outgoing connections are occupied after 40 days!
Why is the Erebus attack stealthy?

• No route manipulation (e.g., BGP hijacking) needed
=> Invisible to control-plane monitors (e.g., BGP collectors)

• Only low rate data-plane attack traffic (520 bit/s or 2 IP/s) is required
=> Difficult to distinguish from legitimate traffic
Who can launch the Erebus attack?

• To attack a targeted node, Erebus attacker needs:
  ✓ **millions** shadow IP addresses
  ✓ **several weeks** of attack execution

• **All Tier-1** networks
  ✓ AT&T, CenturyLink, NTT, ...
  ✓ Can target **any** Bitcoin node!

• Many **large Tier-2** networks
  ✓ Singtel, China Telecom, ...
  ✓ Can target the **majority** of nodes!

• **Nation-state** adversaries
  ✓ Some countries are believed to have direct control over their ISPs

New Report: **North Korean Hackers Stole Funds From South Korean Cryptocurrency Exchanges**
US cybersecurity firm Recorded Future has released a new report linking Lazarus, a North Korean hacking group, to various South Korean cryptocurrency exchange hacking attacks and security breaches.
What about other cryptocurrencies?

- Bitcoin peer-to-peer networking stack is **widely replicated**
  - Erebus attack also applies on **34 out of top-100** cryptocurrencies

All vulnerable!
Countermeasures against the Erebus attack

• The Erebus attack exploits the topological advantage of being large ISPs, not any specific bugs => Hard to counter against!

Partial solutions are available.

Carefully evaluations are needed before deployment.

• Partial solutions:
  ✓ Table size reduction
  ✓ More outgoing connections
  ✓ Incorporating AS topology in the peer selection
  ✓ Protecting peers providing fresher block data
Conclusions

• Erebus attack can isolate Bitcoin nodes in a **stealthy** manner
  ✓ **Low rate** attack traffic (520 bit/s per node)
  ✓ Patiently waiting for a **few weeks**
  ✓ Large ISPs can launch this attack against latest Bitcoin Core

• Mitigating the Erebus attack is **hard**
  ✓ **No** software bugs was exploited
  ✓ Attackers only exploit the **topological advantages** of being ISPs

• Updates on countermeasures: [https://erebus-attack.comp.nus.edu.sg/](https://erebus-attack.comp.nus.edu.sg/)
Muoi Tran
muoitran@comp.nus.edu.sg

https://erebus-attack.comp.nus.edu.sg/