30th USENIX Security Symposium (**USENIX Security** 2021)
https://**erebus-attack-countermeasures**.github.io/

On the Routing-Aware Peering against Network-Eclipse Attacks in Bitcoin

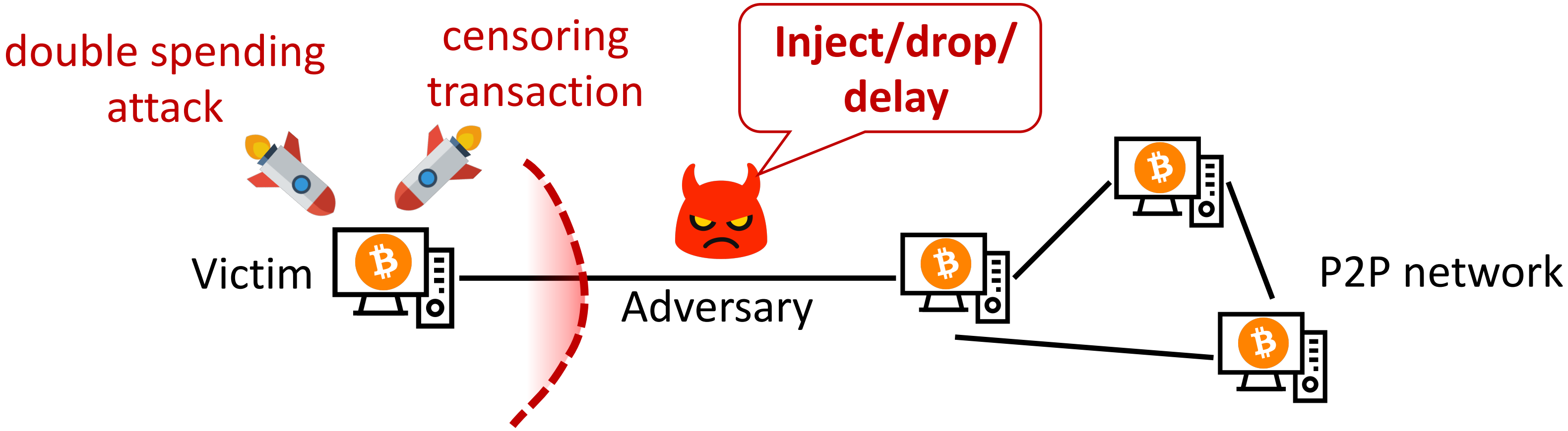
Muoi Tran
NUS

Akshaye Shenoi
NUS

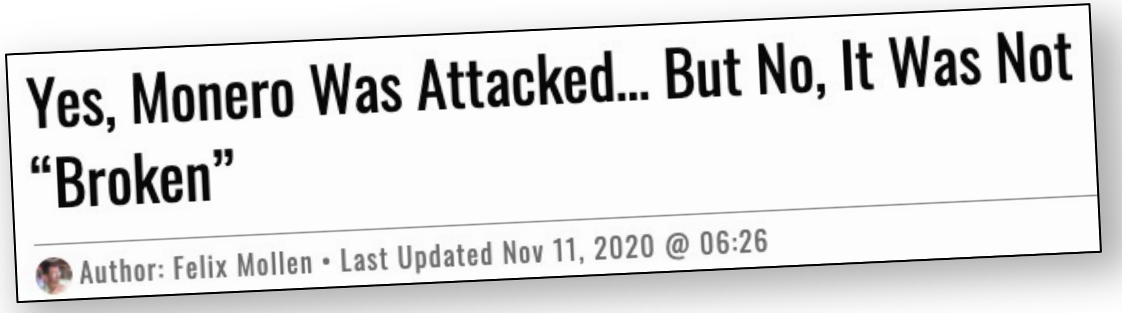
Min Suk Kang
KAIST

Partitioning attacks against blockchain networks are ***threatening***

- ***Isolate*** targeted victim node(s) from the rest of ***P2P network***

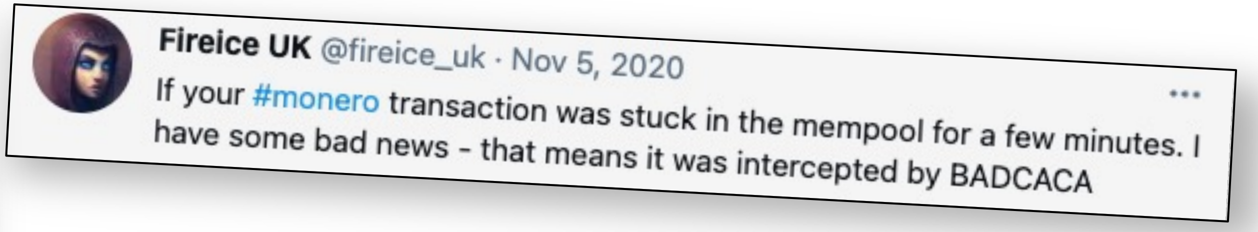


- ***Real eclipse attack*** against Monero network:
  - ✓ Several users had their ***transactions dropped***



Yes, Monero Was Attacked... But No, It Was Not "Broken"

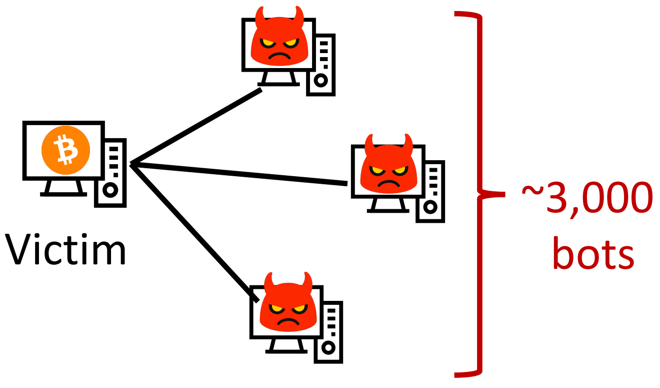
Author: Felix Mollen • Last Updated Nov 11, 2020 @ 06:26



Fireice UK @fireice_uk · Nov 5, 2020

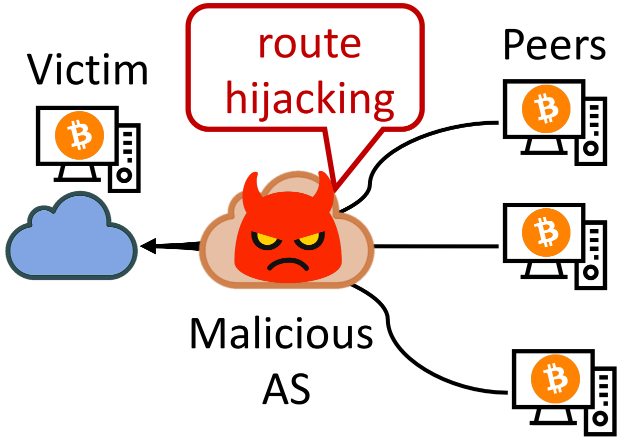
If your #monero transaction was stuck in the mempool for a few minutes. I have some bad news - that means it was intercepted by BADCACA

Most of partitioning attacks have been ***effectively mitigated***



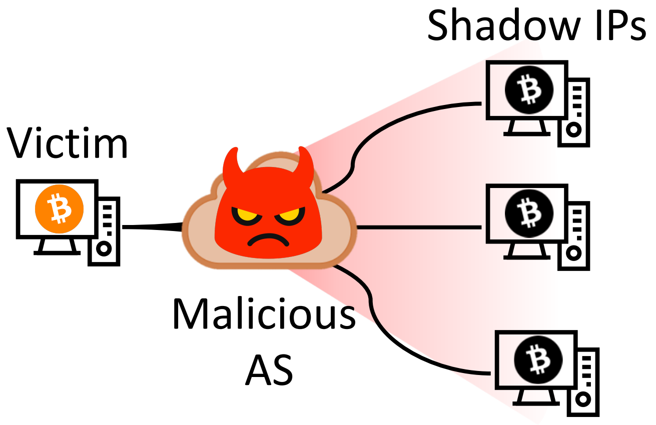
Botnet-based eclipse attack:

- ✓ Heilman et al. *[USENIX Security'15]*
- ✓ Attack is ***impossible*** with up-to-date Bitcoin clients



Route hijacking attack:

- ✓ Apostolaki et al. *[IEEE S&P'17]*
- ✓ Attack is ***detectable*** and ***attributable***

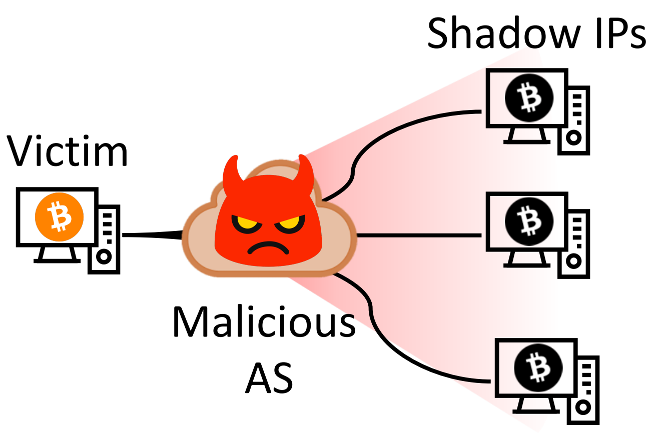


Erebus attack:

- ✓ Tran et al. *[IEEE S&P'20]*
- ✕ Attack is ***stealthier*** and ***harder*** to prevent

Most of partitioning attacks have been ***effectively mitigated*** (cont.)

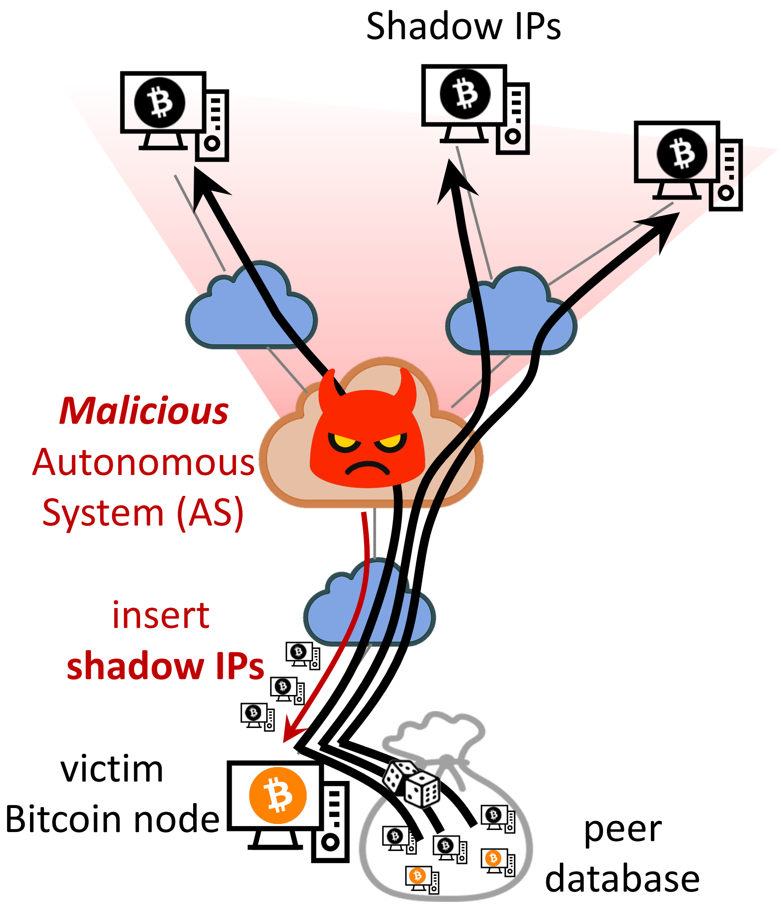
What are practical countermeasures to Erebus attack?



Erebus attack:

- ✓ Tran et al. *[IEEE S&P'20]*
- ✗ Attack is ***stealthier*** and ***harder*** to prevent

Erebus: a "***network-eclipse***" attack in Bitcoin



The ***Erebus attack*** (Tran et al. [IEEE S&P'20])

- Malicious AS ***spoofs*** peer identities using IPs behind herself (a.k.a. ***shadow IPs***)
- Attacker ***slowly inserts*** shadow IPs into victim's database and waits
- Attacker becomes ***the man-in-the-middle*** of all peer connections of the victim

=> Victim is ***eclipsed!***

Countering Erebus is ***challenging***

- ***Network*** adversary exploits the ***permissionless nature*** of Bitcoin P2P:
  ✓***Millions*** of shadow IPs can be found
  => Victim nodes are ***eventually eclipsed*** by shadow IPs!
- Some approaches for ***countermeasures*** against Erebus attacks:

Workaround

VPN

Tor

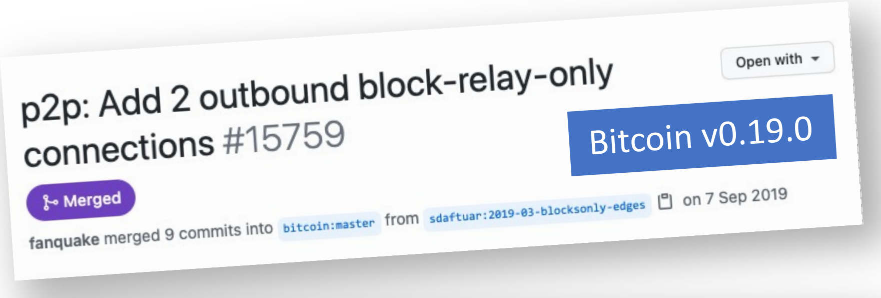
Whitelisting

Relying on external services

Quick fixes

Protocol tweaks

Not complete solutions

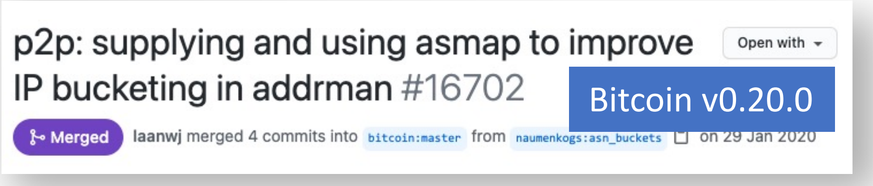


p2p: Add 2 outbound block-relay-only connections #15759

Merged

fanquake merged 9 commits into bitcoin:master from sdaftuar:2019-03-blocksonly-edges on 7 Sep 2019

Bitcoin v0.19.0



p2p: supplying and using asmap to improve IP bucketing in addrman #16702

Merged

laanwj merged 4 commits into bitcoin:master from naumenkogs:asn_buckets on 29 Jan 2020

Bitcoin v0.20.0

Countering Erebus is ***challenging*** (cont.)

- ***Network*** adversary exploits the ***permissionless nature*** of Bitcoin P2P:
  - ✓***Millions*** of shadow IPs can be found
    => Victim nodes are ***eventually eclipsed*** by shadow IPs!
- Some approaches for ***countermeasures*** against Erebus attacks:

Workaround

VPN

Tor

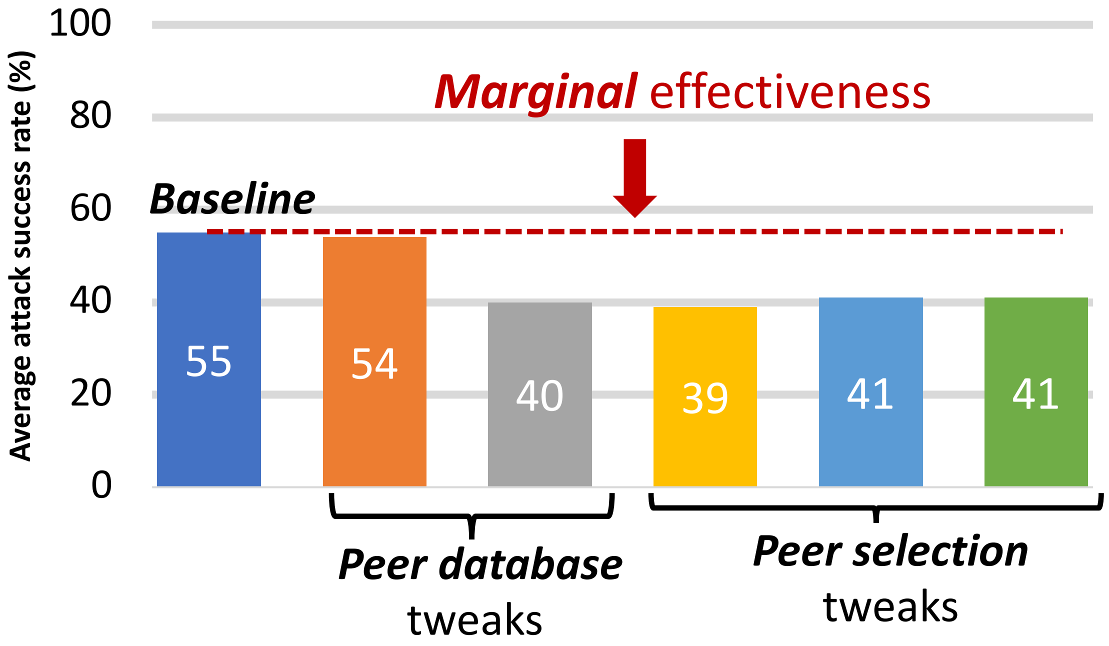
Whitelisting

Relying on external services

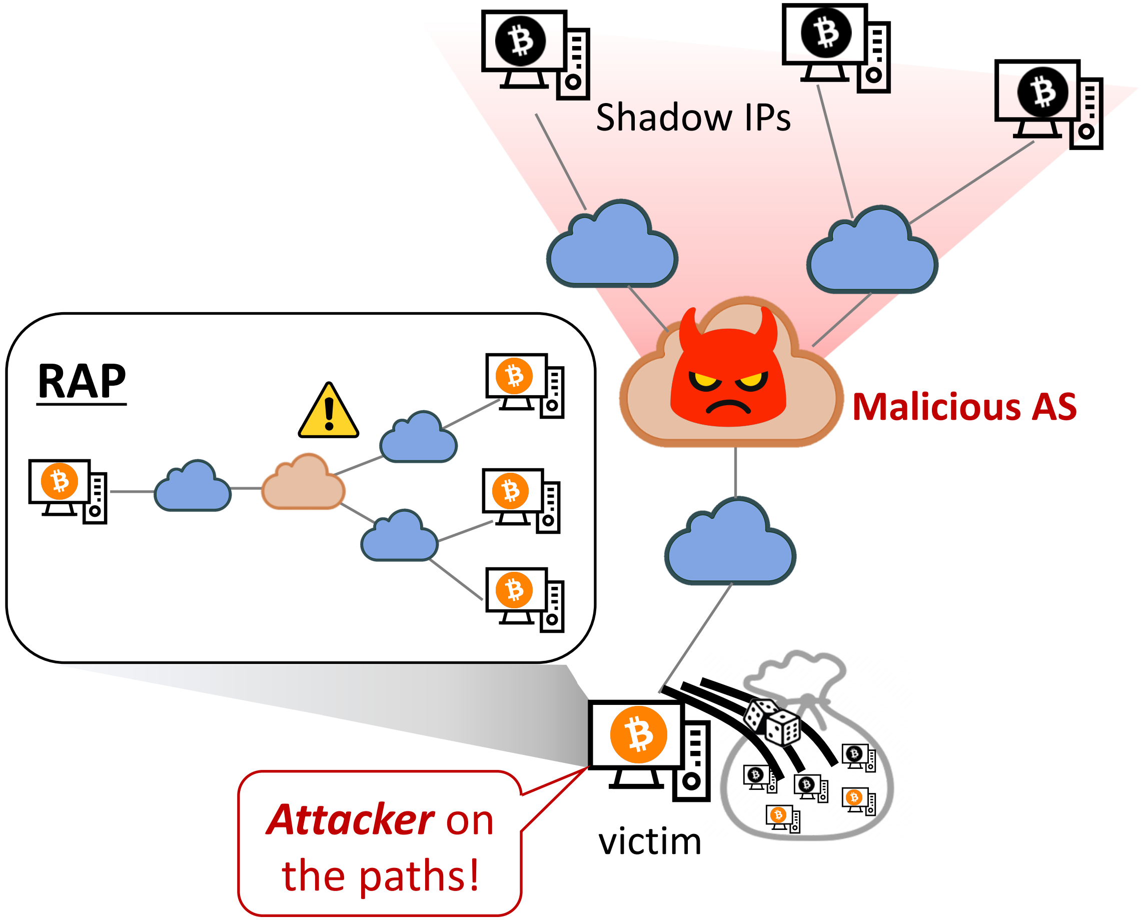
Quick fixes

Protocol tweaks

Not complete solutions



A *known* solution to network-based attacks: *Route-Aware Peering*

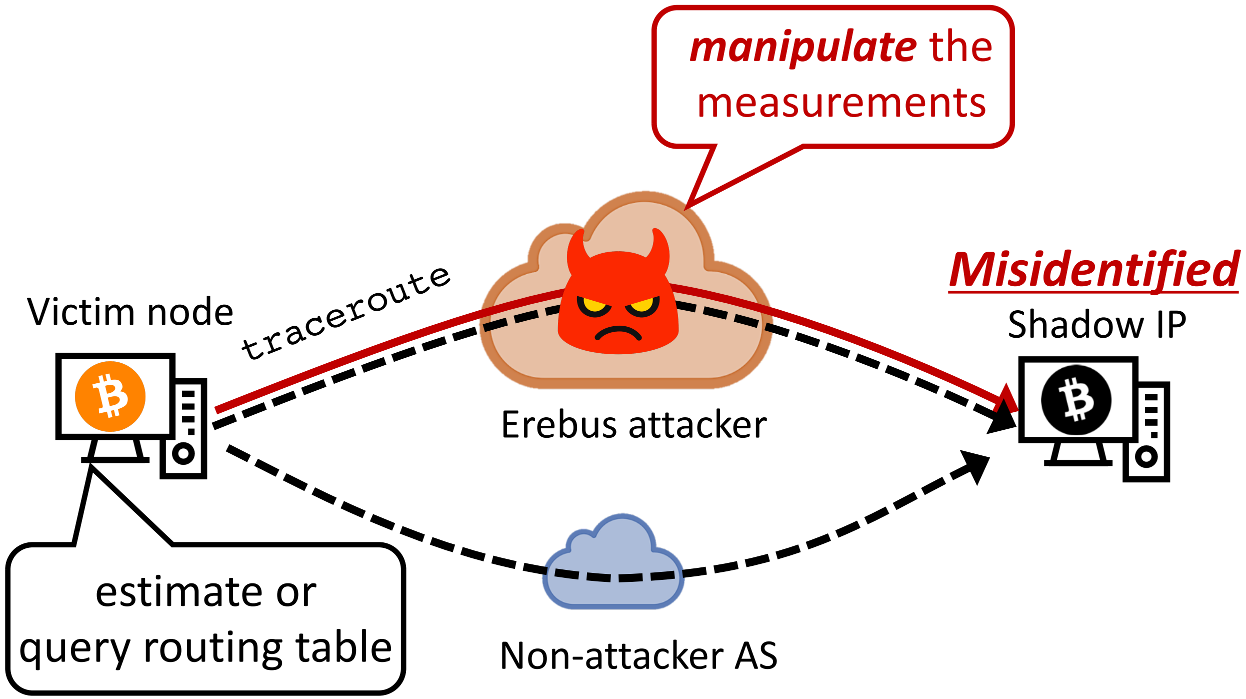


Attacker on the paths!

- ***Route-Aware Peering*** (RAP):
  - ✓is ***frequently used*** to avoid on-path network adversaries:
    - ❖**LASTor** *[IEEE S&P'12]*
    - ❖**Counter-RAPTOR** *[IEEE S&P'17]*
    - ❖...
  - ✓peers are selected based on the ***routing paths*** to the peers

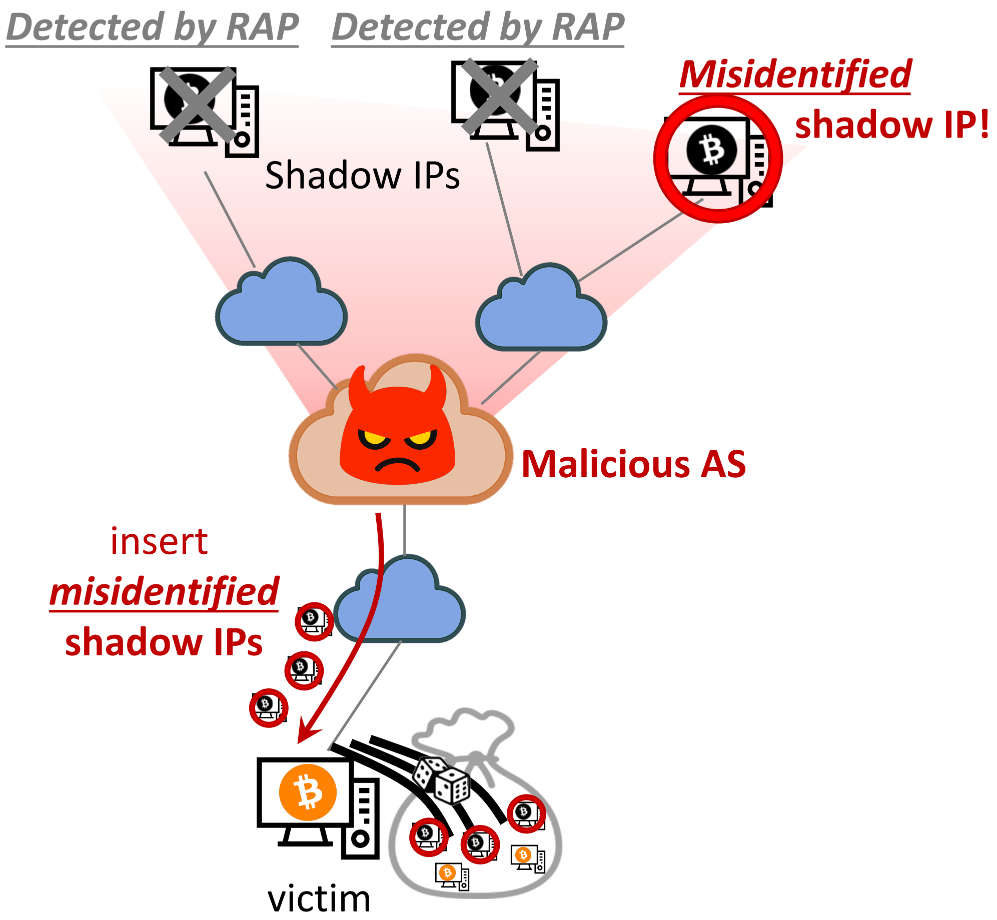
Can RAP ***prevent*** Erebus attacks? ***No***, we found a ***subtle*** problem!

The Devil is in the details:
Non-idealities of RAP implementations



- RAP can get the ***routing paths*** to the peers by:
  - ~~✓ ***Measuring*** the ***traffic*** routes~~
  - ~~=> Results can be ***manipulated!***~~
  - ✓ ***Estimating*** the ***forwarding*** routes
  - => Shadow IPs can be ***misidentified!***
- Misidentified shadow IPs can be ***exploited*** by ***RAP-aware*** Erebus!

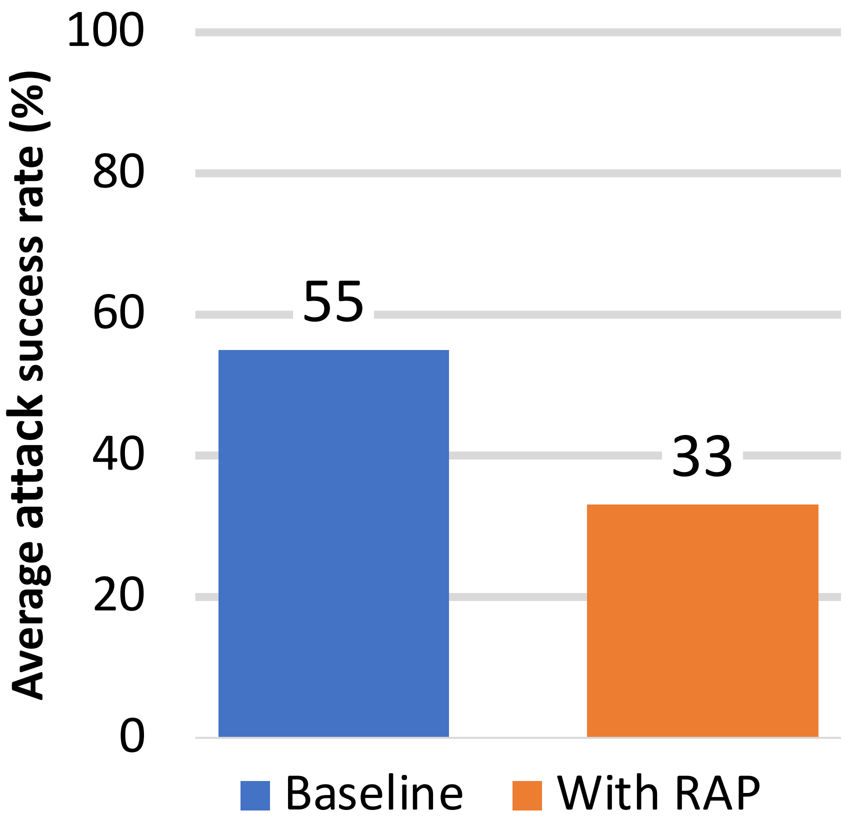
Smarter attacker uses ***only misidentified shadow IPs***



- Attacker selects misidentified shadow IPs ***in advance***
  - ✓By ***emulating*** the best RAP implementation by the victim

=> Insert ***only*** misidentified shadow IPs

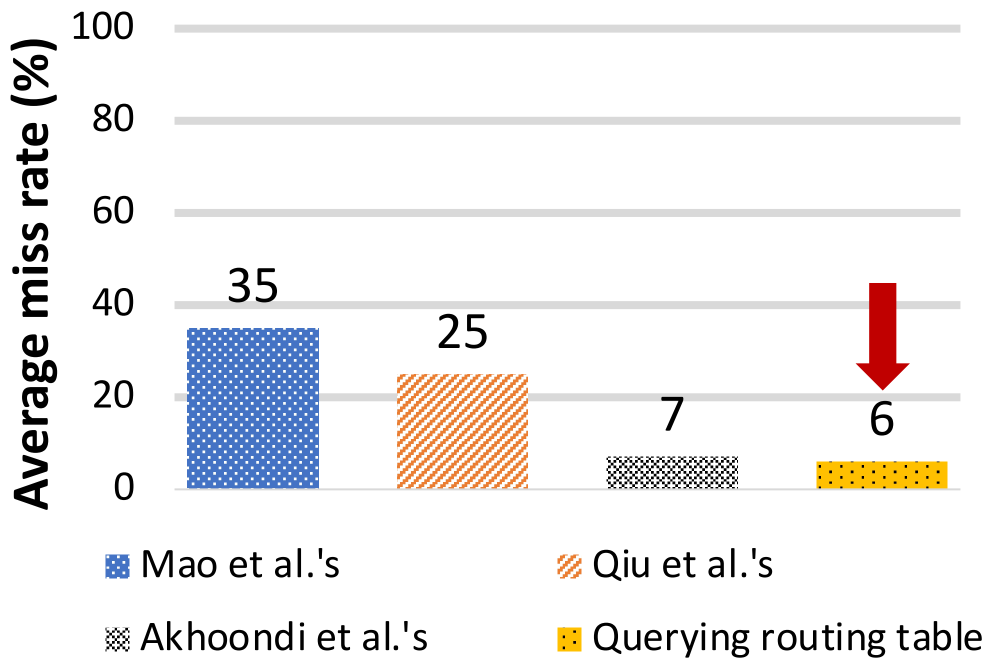
Can RAP ***prevent*** this smarter Erebus?

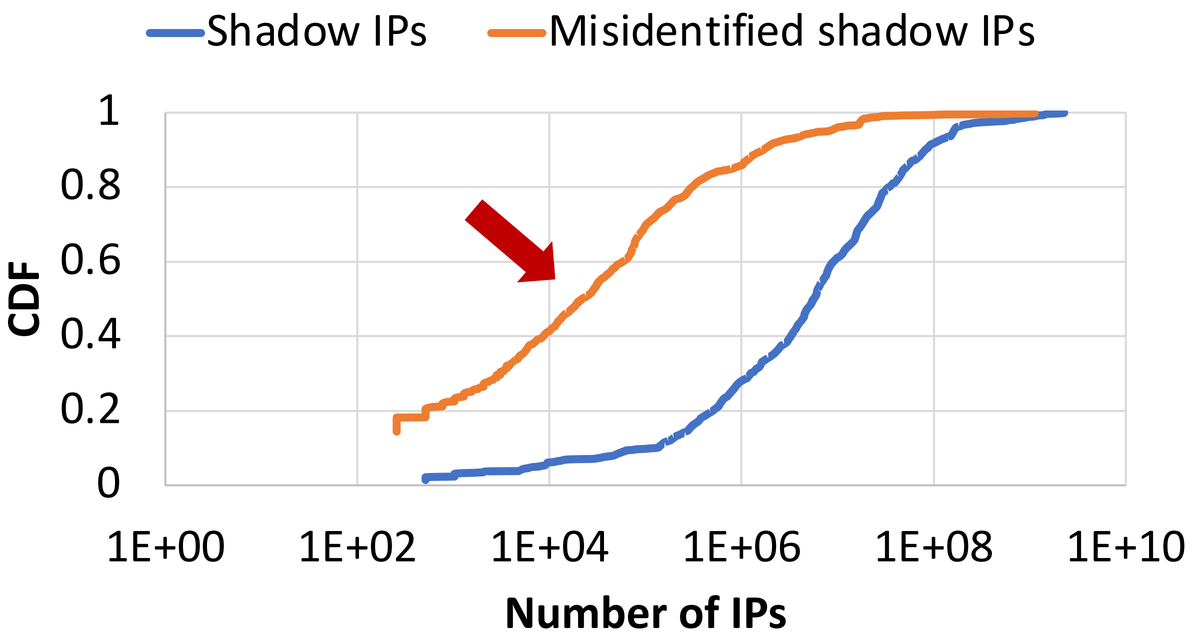


- Experiment setup:
  - ✓ ***~6,000*** attack scenarios
  - ✓ Attacker: ***top-100 ASes***
  - ✓ Victim: ***59 locations globally***
    - ❖ popular cloud networks

RAP alone is ***insufficient***!

Why does RAP ***not work*** in Bitcoin?



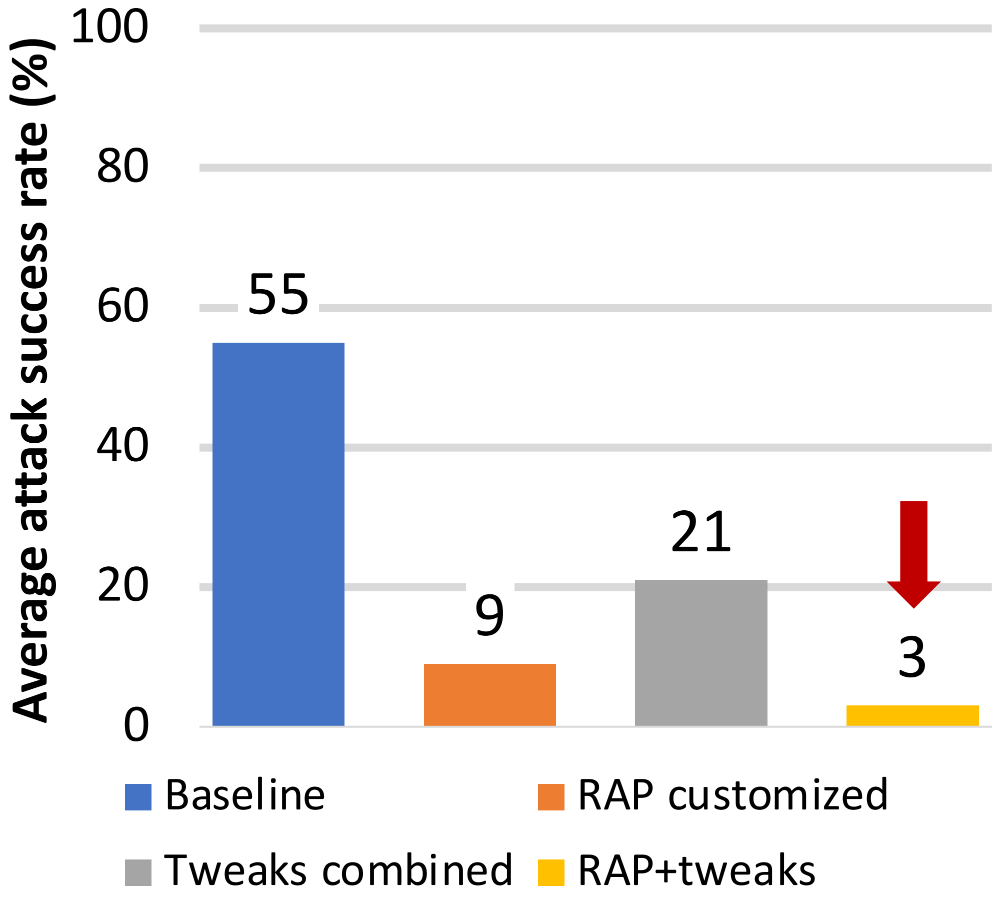


- Even ***state-of-the-art*** route estimation implementations are ***imperfect***

=> ***At least 6%*** of shadow IPs are ***misidentified!***

=> Attacker can easily find ***tens of thousands*** of spoofed peer identities!

Making the best of available solutions



- RAP must be ***customized*** to each Bitcoin node's ***topology location*** (please see our paper for details)

- ***Extensive evaluation*** for ***all*** possible combination of tweaks is needed

- RAP + tweaks is ***the most effective*** defense (***so far***)

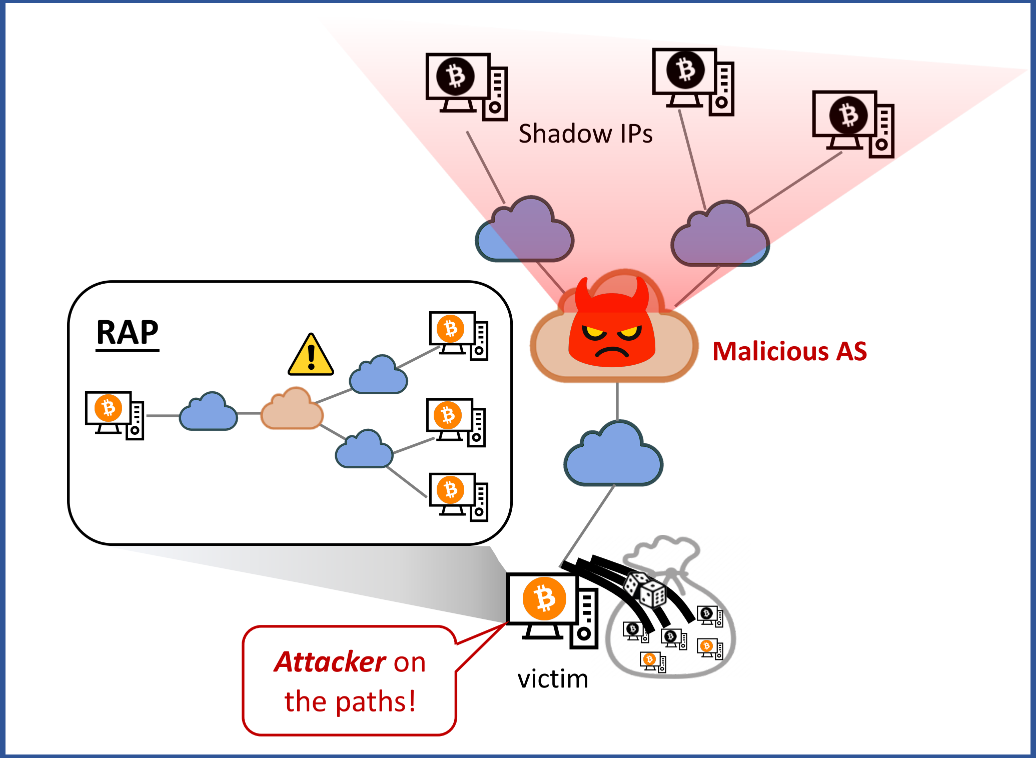
Conclusions

- Routing-Aware Peering (RAP) alone is ***insufficient*** to prevent Erebus:
  - ✓***No perfect, error-free*** route estimation for RAP in practice
  - ✓***Smarter*** Erebus attacker can exploit RAP's weakness

- ***Most*** Bitcoin nodes ***can be protected*** from Erebus attacks:
  - ✓RAP must be ***customized*** for each node
  - ✓RAP must be ***combined*** with available protocol tweaks

- Updates on ***deployments*** of RAP and other protocol tweaks: https://erebus-attack-countermeasures.github.io/

https://erebus-attack-countermeasures.github.io/



Muoi Tran

muoitran@comp.nus.edu.sg

NUS National University of Singapore

KAIST