IEEE Symposium on Security and Privacy (**IEEE S&P**) 2020

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

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

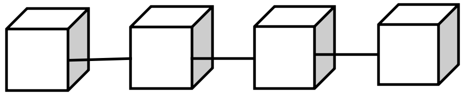
NUS National University of Singapore

EREBUS

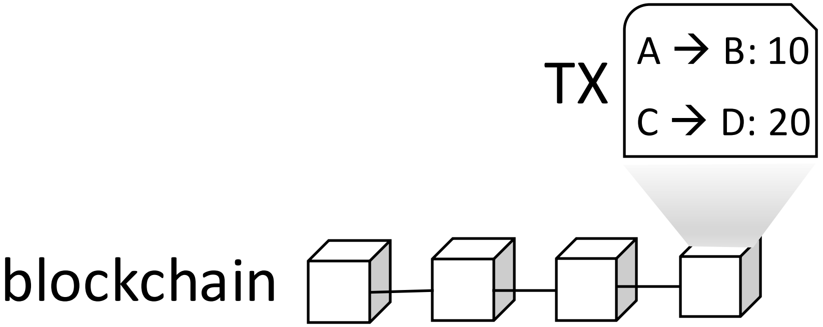
Bitcoin relies on underlying ***peer-to-peer*** network

Bitcoin relies on underlying ***peer-to-peer*** network

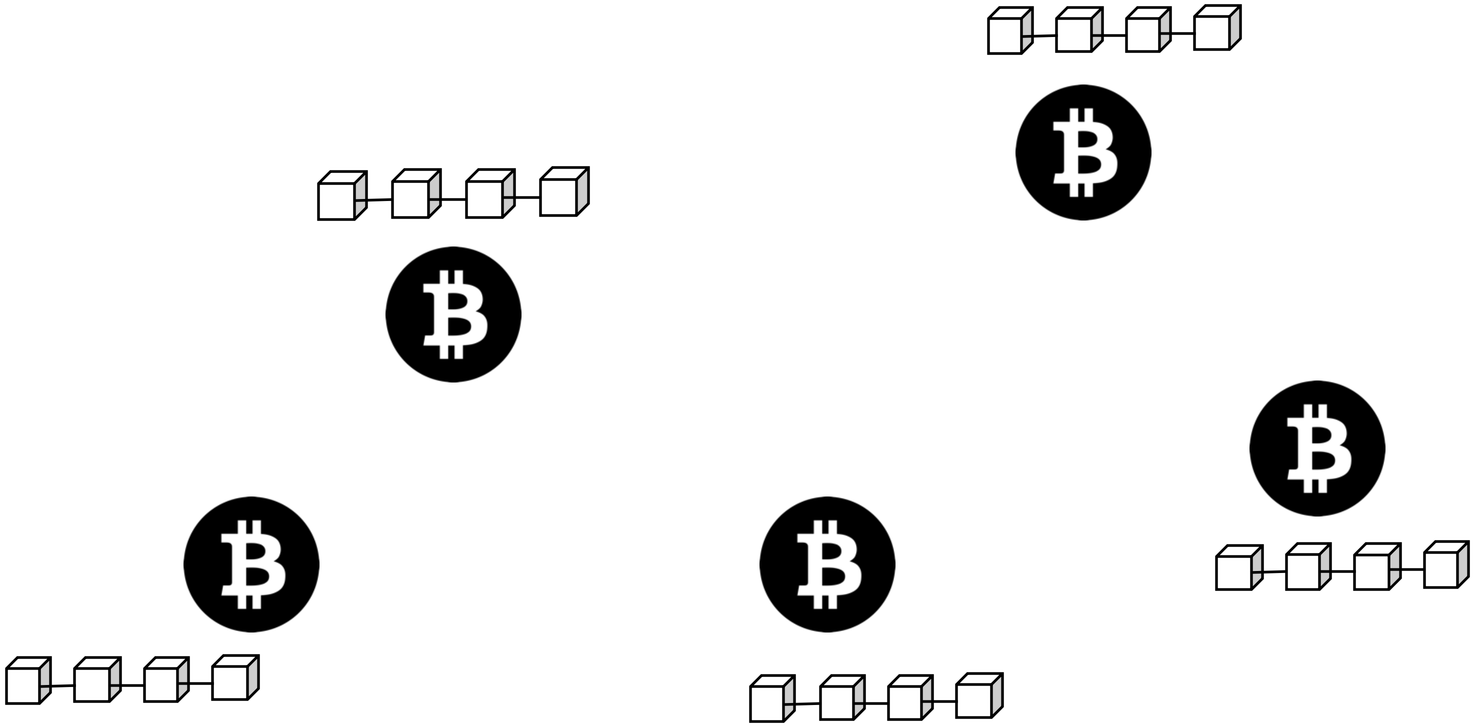
blockchain



Bitcoin relies on underlying ***peer-to-peer*** network

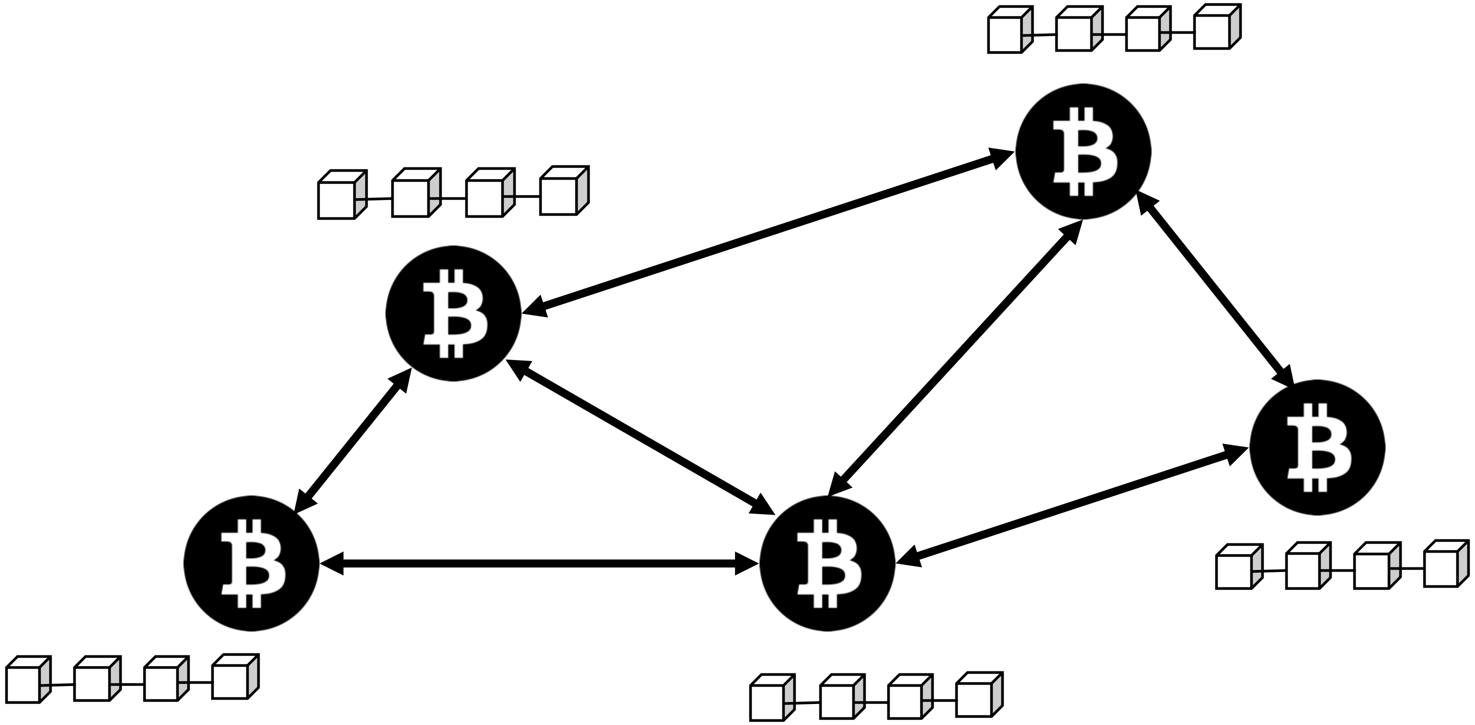


Bitcoin relies on underlying ***peer-to-peer*** network

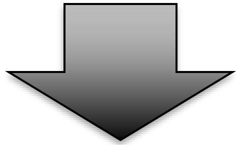


Bitcoin consensus rules

Bitcoin relies on underlying ***peer-to-peer*** network

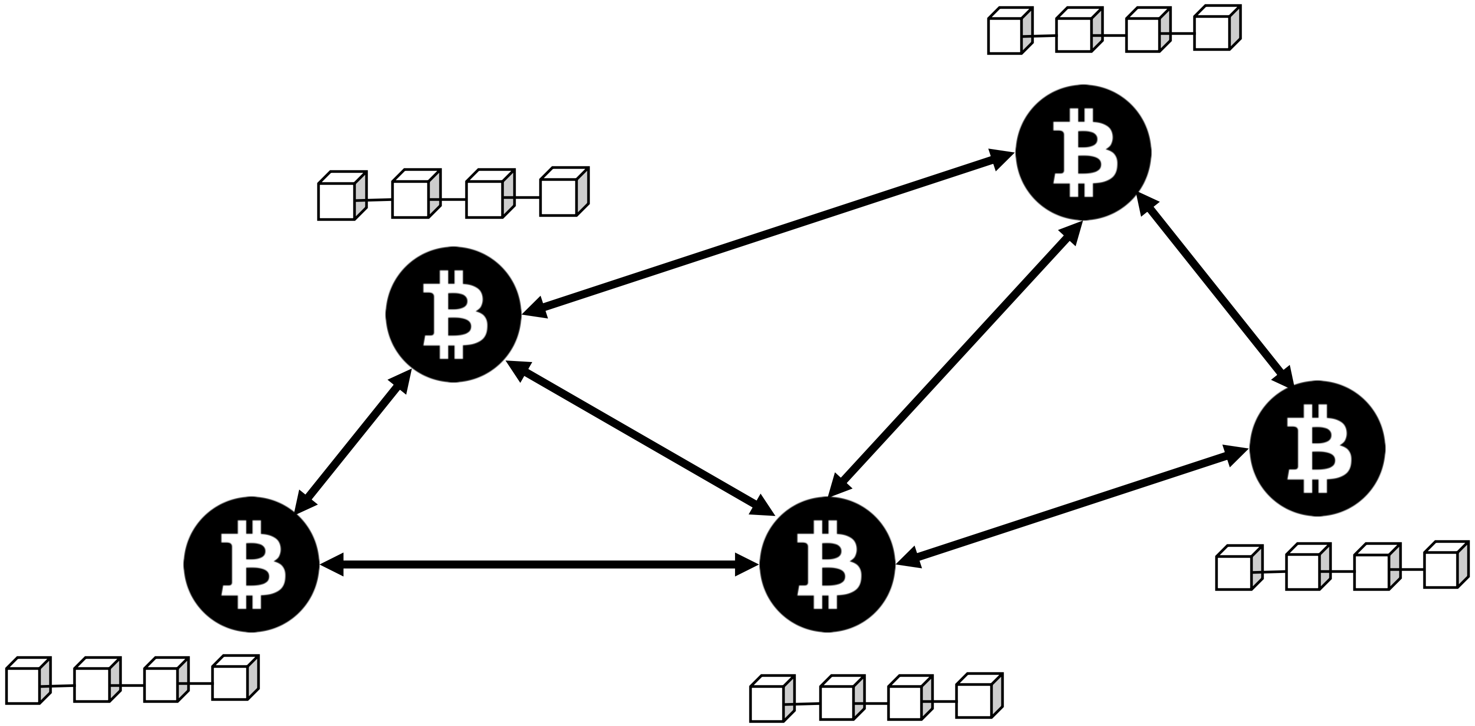


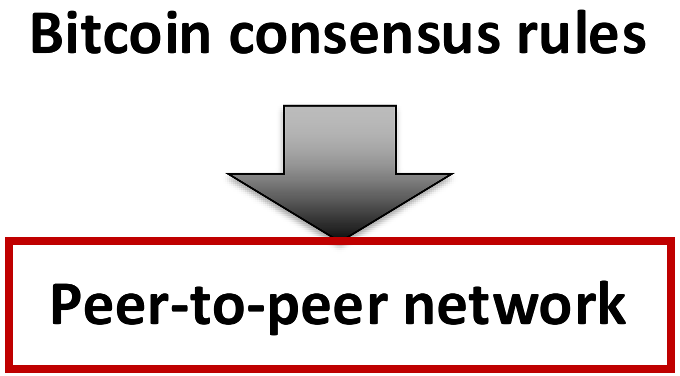
Bitcoin consensus rules



Peer-to-peer network

Bitcoin relies on underlying ***peer-to-peer*** network

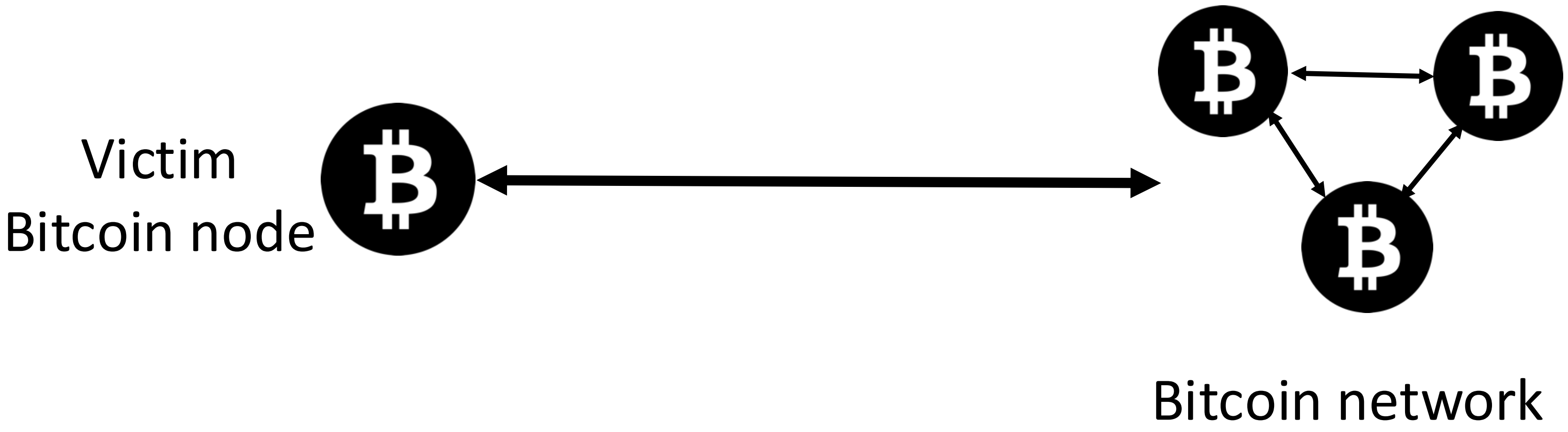




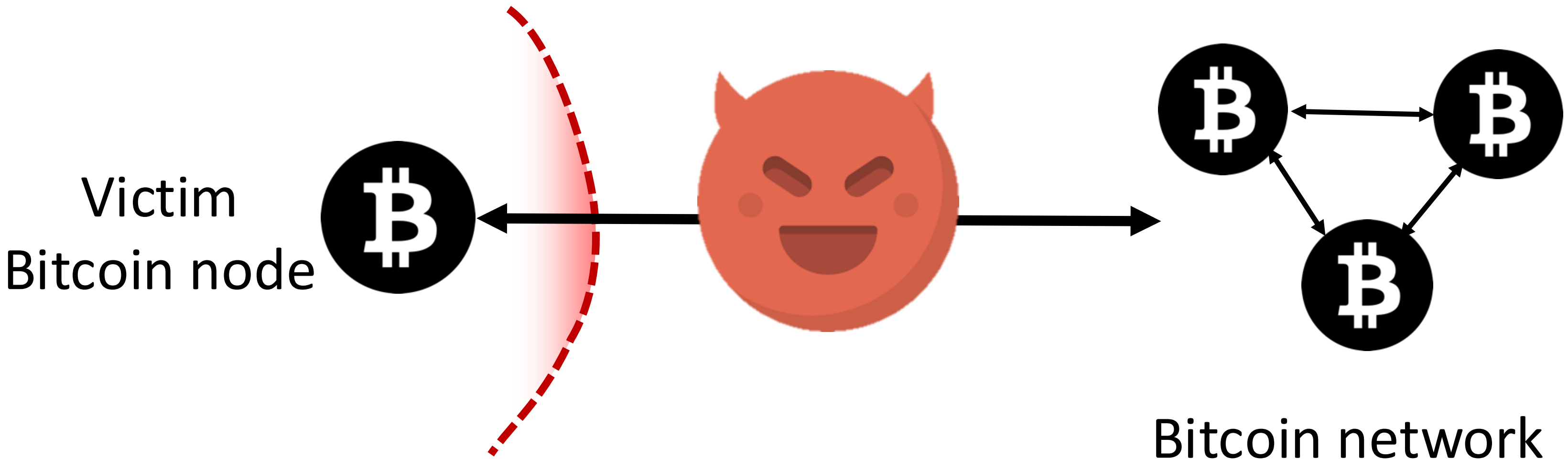
Bitcoin consensus rules

Peer-to-peer network

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

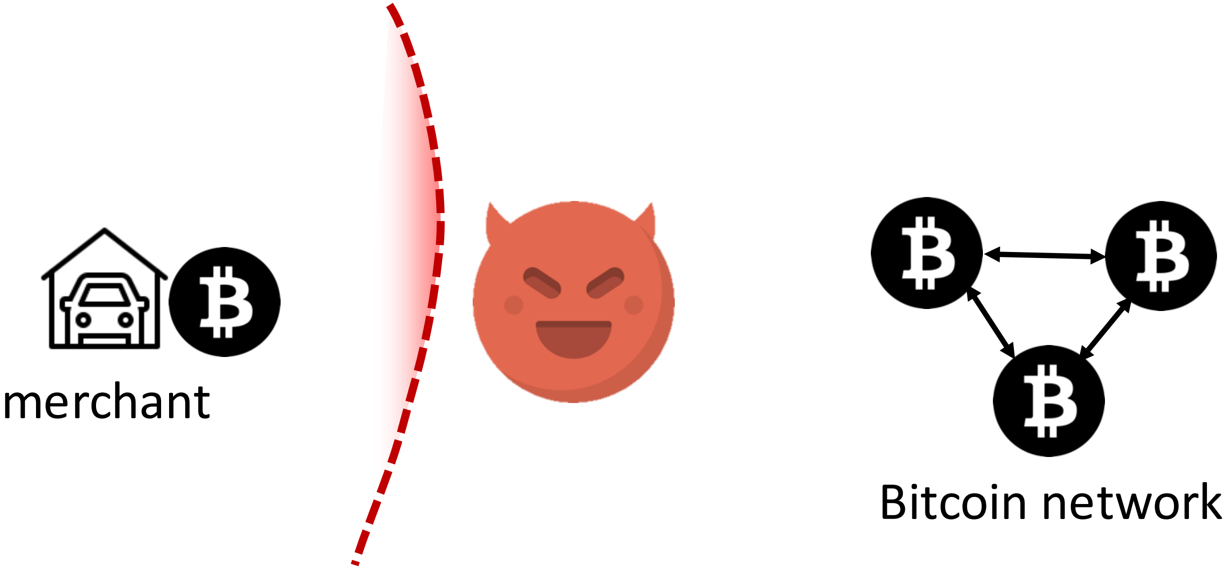


Bitcoin peer-to-peer network can be ***partitioned***

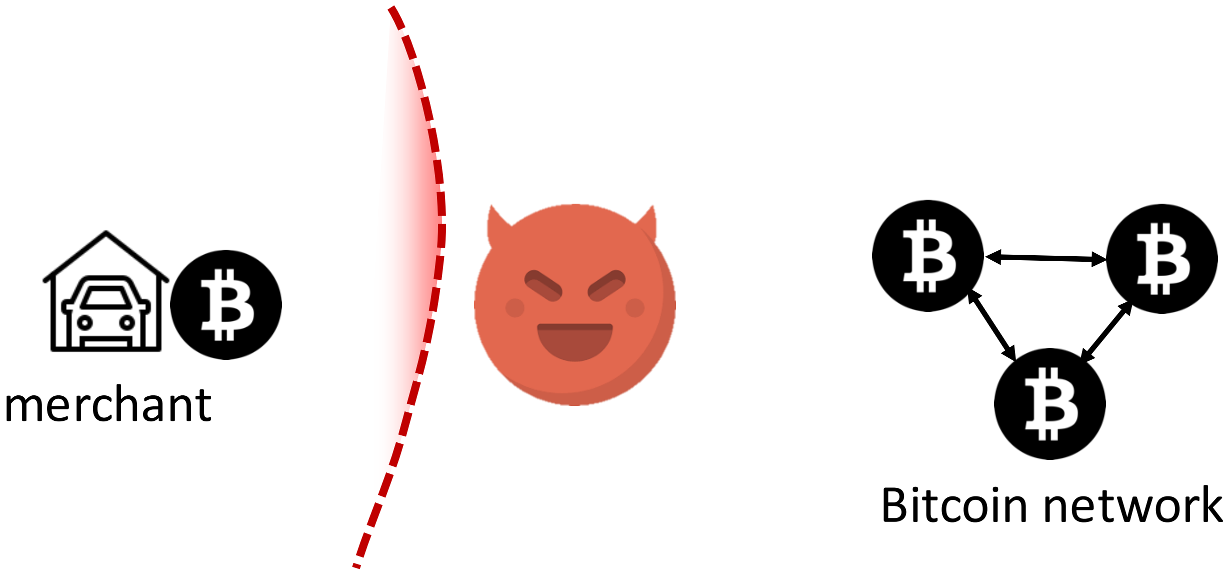


Partitioning attacks: isolate victim node(s) from the rest of network

Partitioning attack is a ***dangerous*** threat

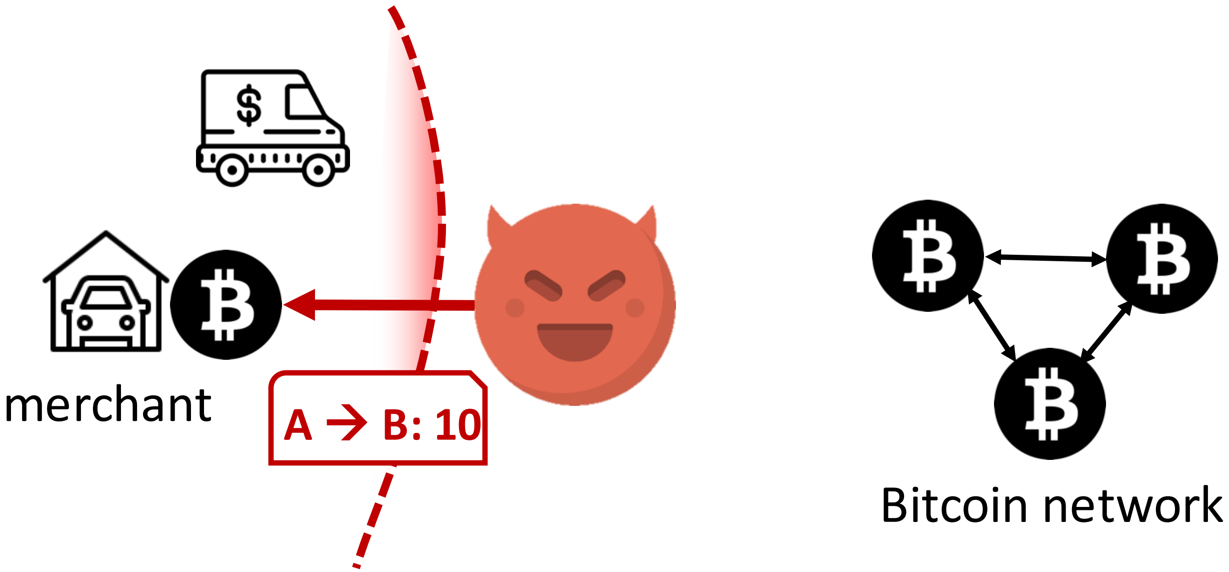


Partitioning attack is a ***dangerous*** threat



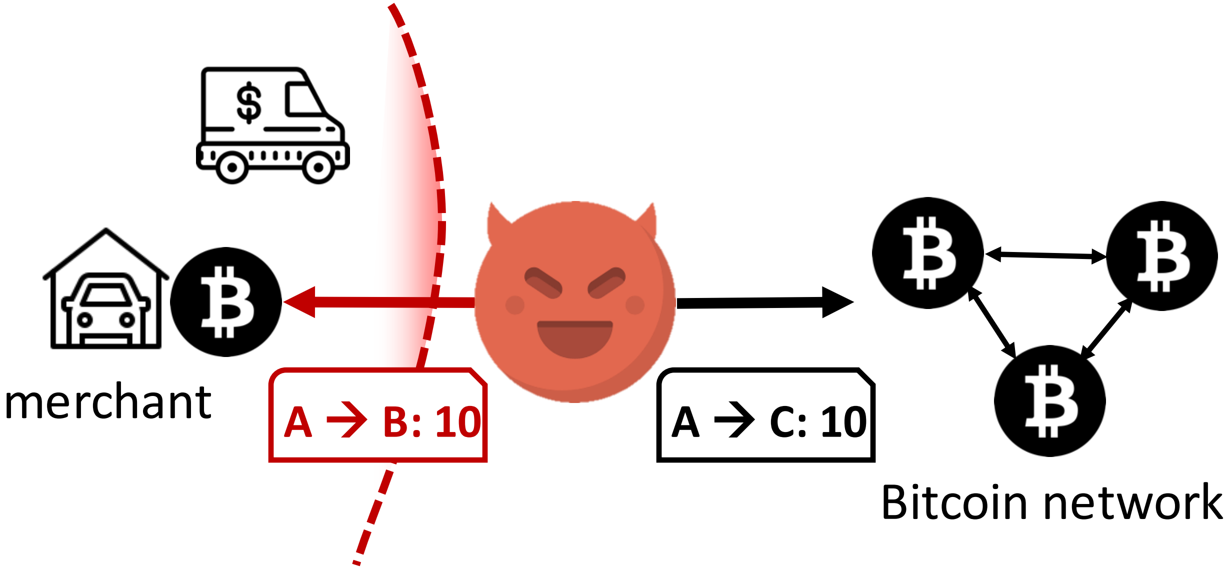
Example: ***Double spending*** attack

Partitioning attack is a ***dangerous*** threat



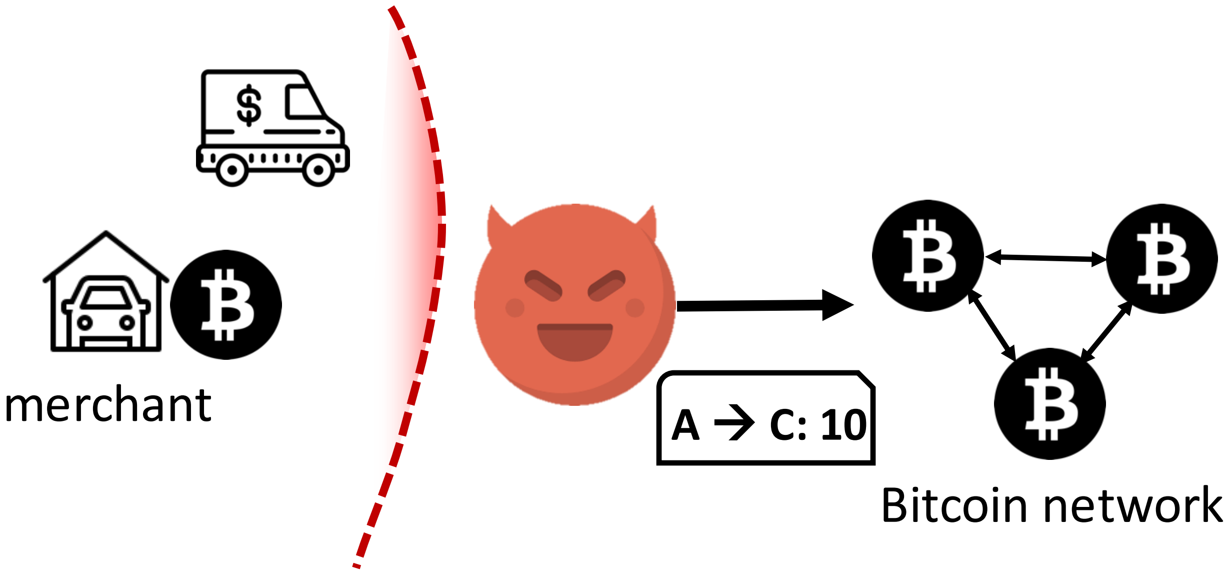
Example: ***Double spending*** attack

Partitioning attack is a ***dangerous*** threat



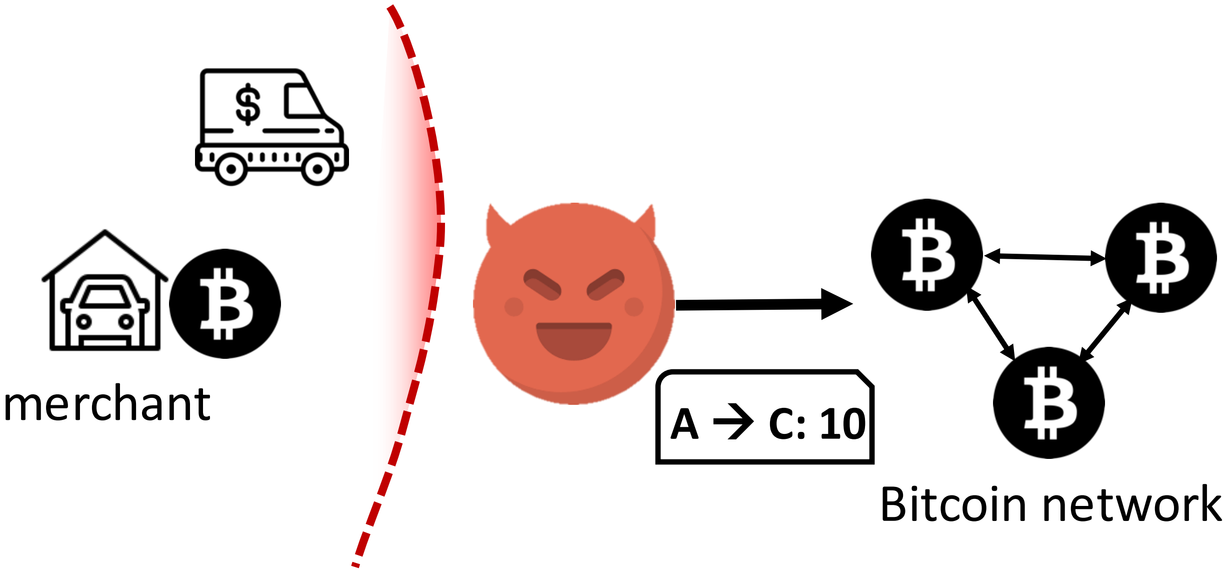
Example: ***Double spending*** attack

Partitioning attack is a ***dangerous*** threat



Example: ***Double spending*** attack

Partitioning attack is a ***dangerous*** threat

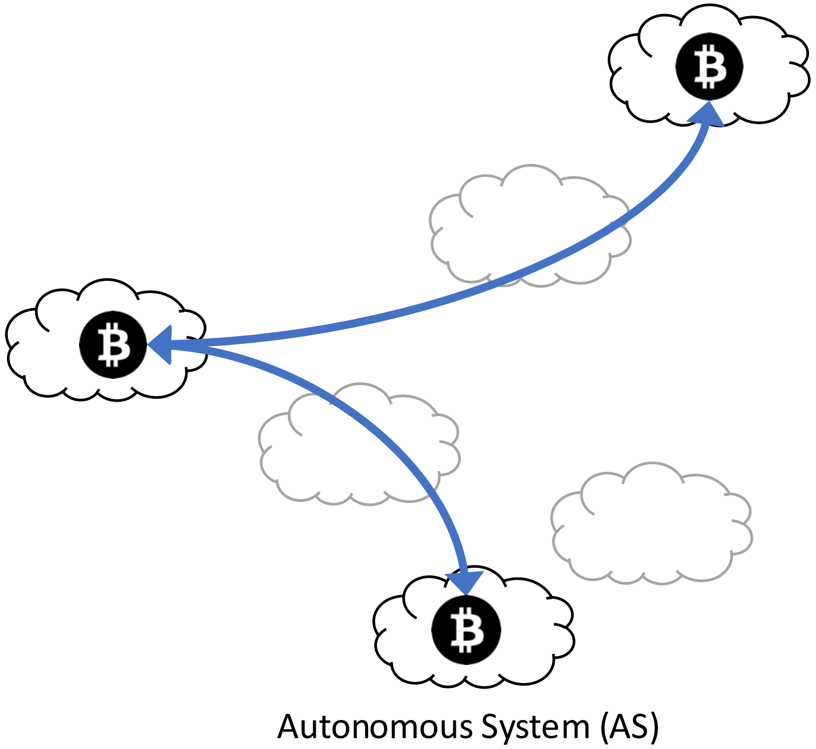


Partitioning ***enables/improves*** several other attacks:

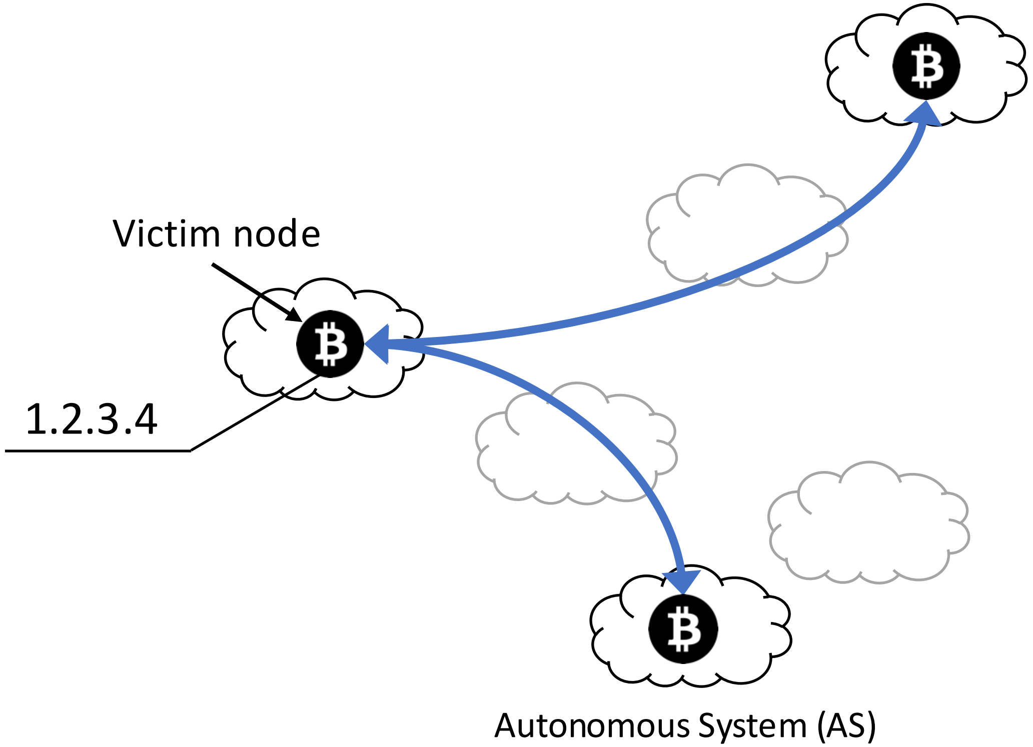
- ✓ 51% attack
- ✓ selfish mining
- ✓ censoring transactions
- ✓ take down cryptocurrencies
- ✓ …

Example: ***Double spending*** attack

Previous attack: ***routing manipulation*** to partition Bitcoin’s peer-to-peer network

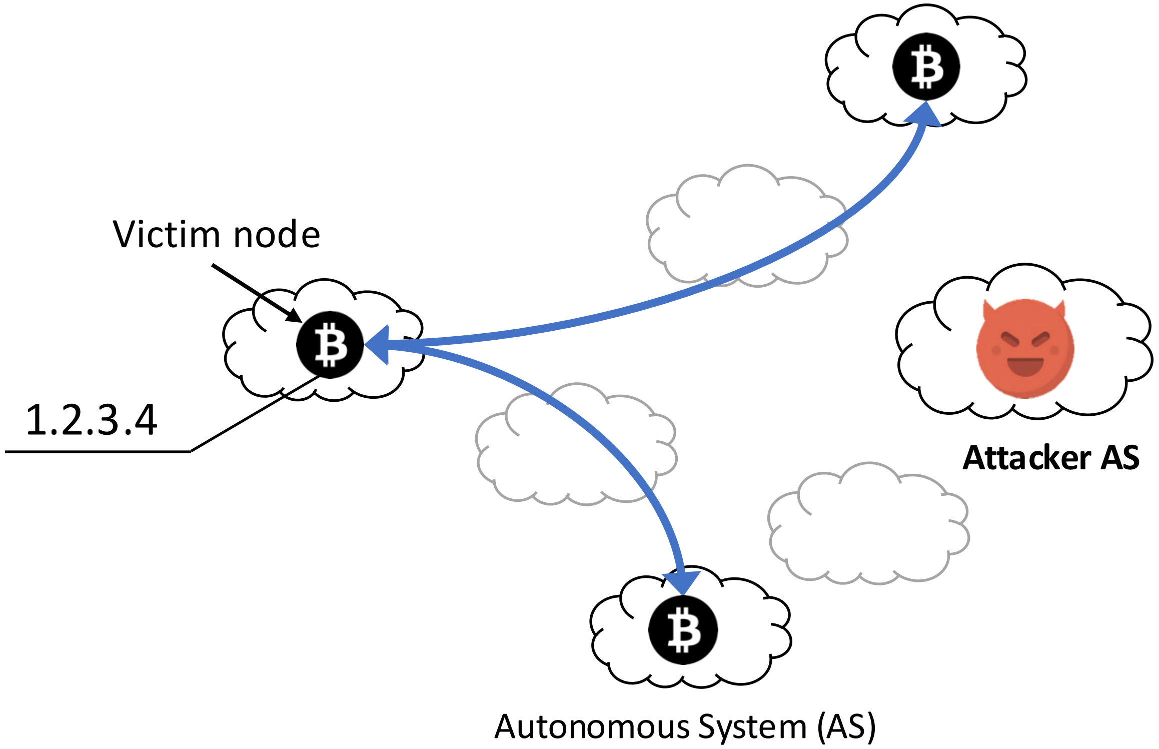


Previous attack: ***routing manipulation*** to partition Bitcoin's peer-to-peer network



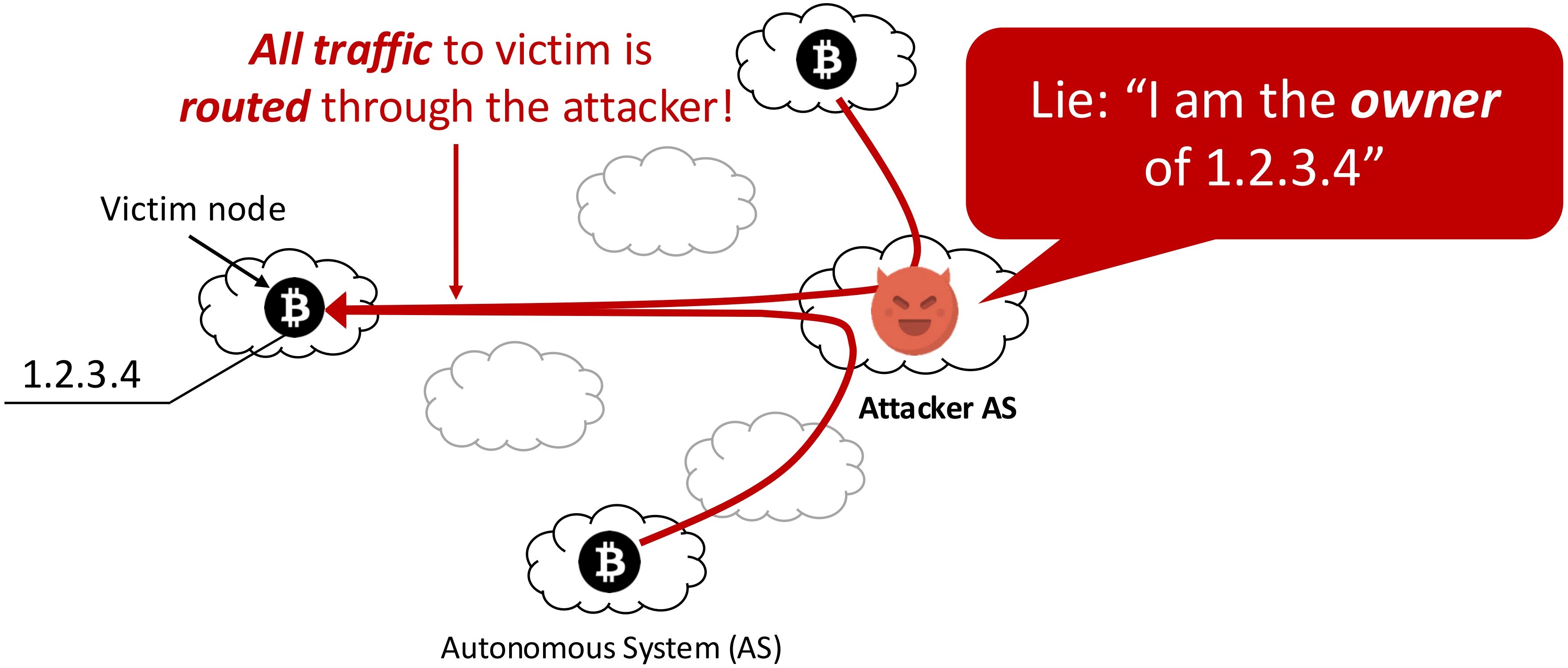
- Bitcoin hijacking (Apostolaki et al., **IEEE S&P'17**)

Previous attack: ***routing manipulation*** to partition Bitcoin's peer-to-peer network



- Bitcoin hijacking (Apostolaki et al., **IEEE S&P'17**)
  - ✓ Attacker AS uses ***BGP hijacking*** to hijack victim connections

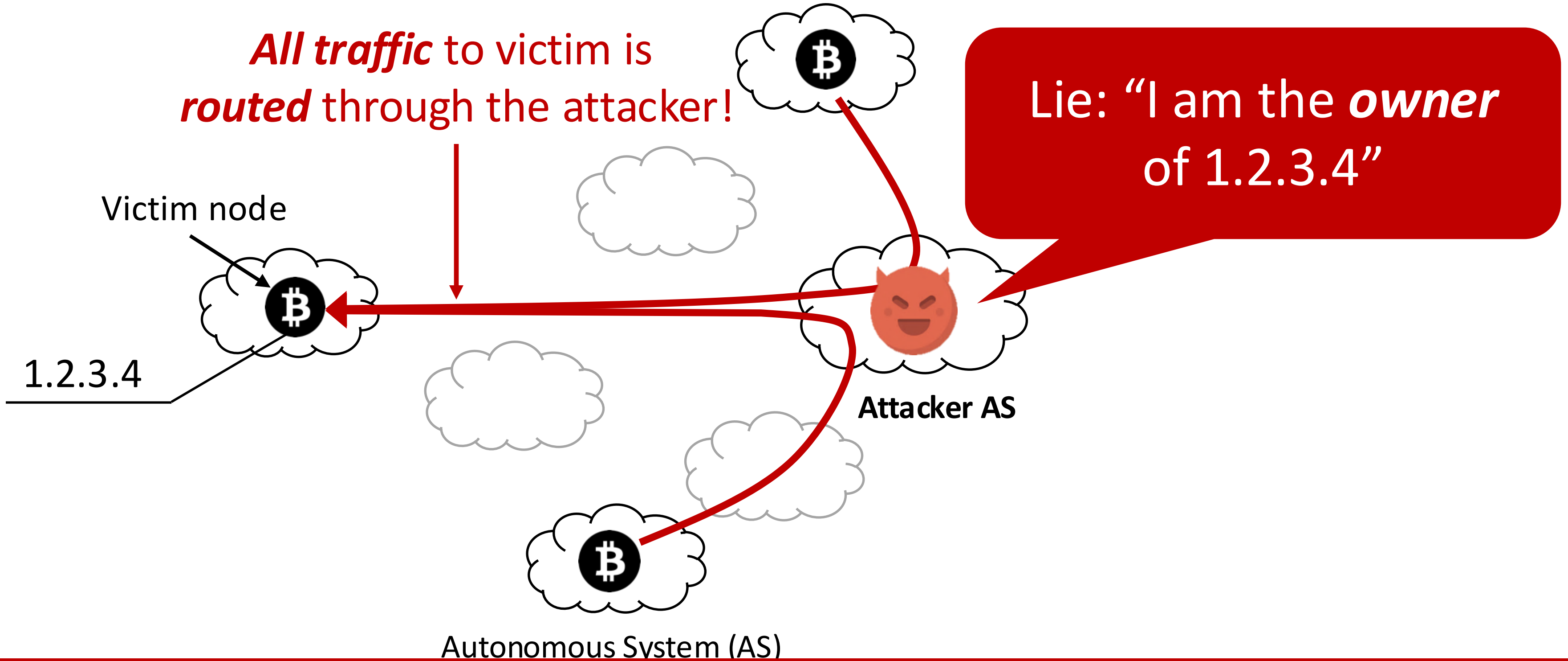
Previous attack: ***routing manipulation*** to partition Bitcoin's peer-to-peer network



All traffic to victim is ***routed*** through the attacker!
Lie: "I am the ***owner*** of 1.2.3.4"
Victim node
1.2.3.4
Attacker AS
Autonomous System (AS)

- Bitcoin hijacking (Apostolaki et al., **IEEE S&P'17**)
  - ✓ Attacker AS uses ***BGP hijacking*** to hijack victim connections

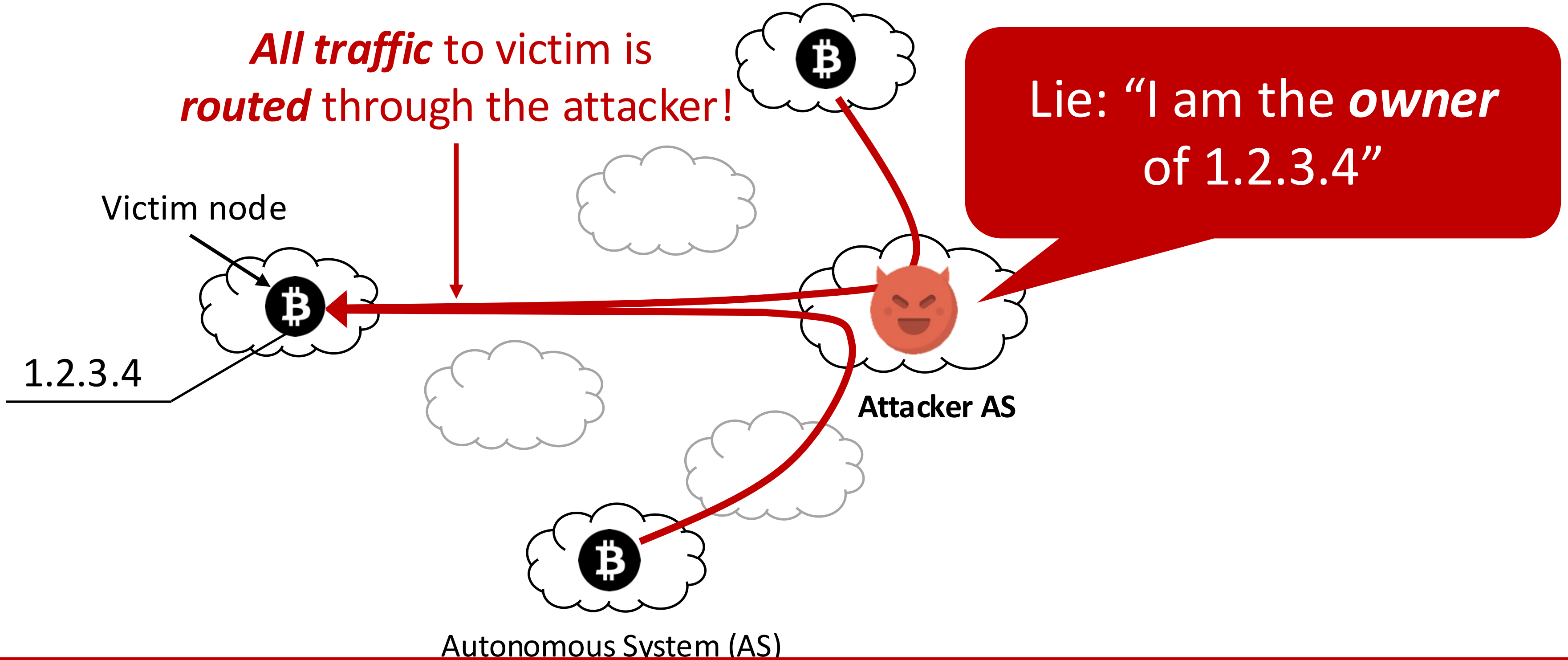
Previous attack: ***routing manipulation*** to partition Bitcoin's peer-to-peer network



All traffic to victim is
routed through the attacker!
Victim node
1.2.3.4
Lie: "I am the ***owner*** of 1.2.3.4"
Attacker AS
Autonomous System (AS)

ASes (e.g., large ISPs) *can* do it.

Previous attack: ***routing manipulation*** to partition Bitcoin's peer-to-peer network

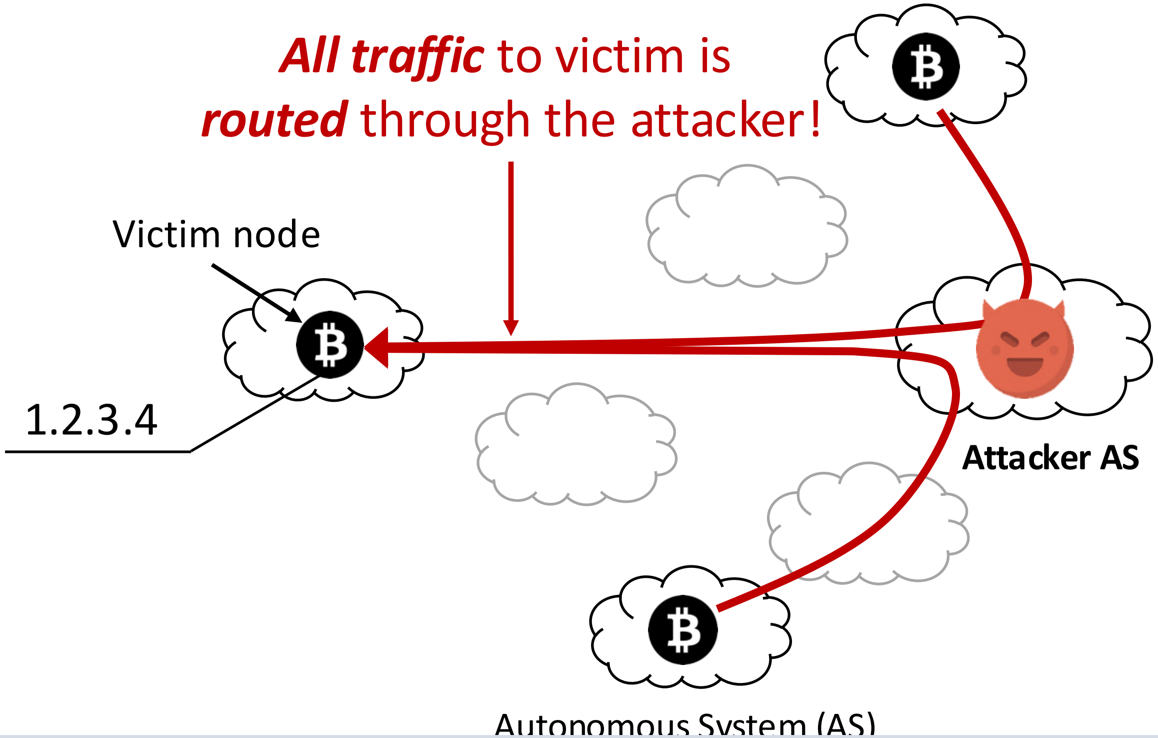


All traffic to victim is ***routed*** through the attacker!
Victim node
1.2.3.4
Lie: "I am the ***owner*** of 1.2.3.4"
Attacker AS
Autonomous System (AS)

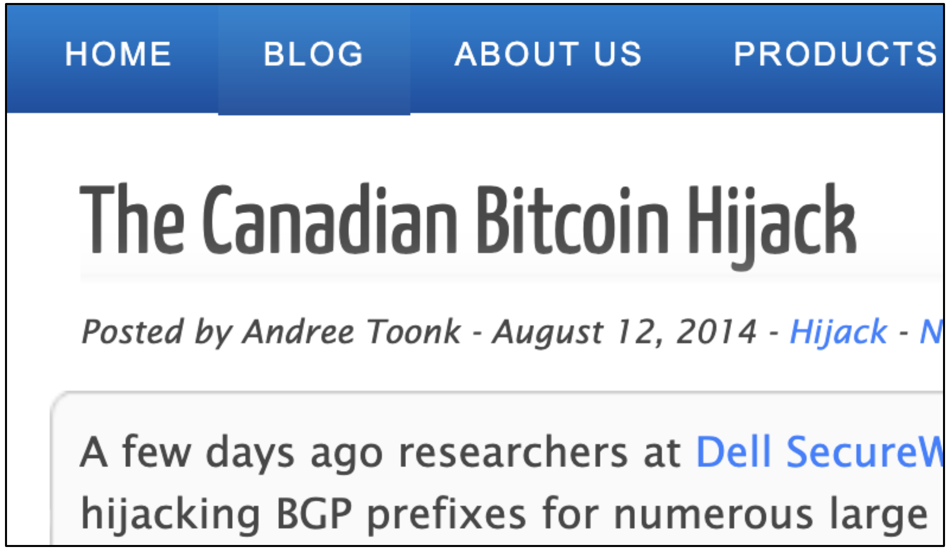
ASes (e.g., large ISPs) <u>*can*</u> do it.

✓ **Question: " *Do they really launch this attack in practice?*"**

Previous attack: ***routing manipulation*** to partition Bitcoin's peer-to-peer network



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



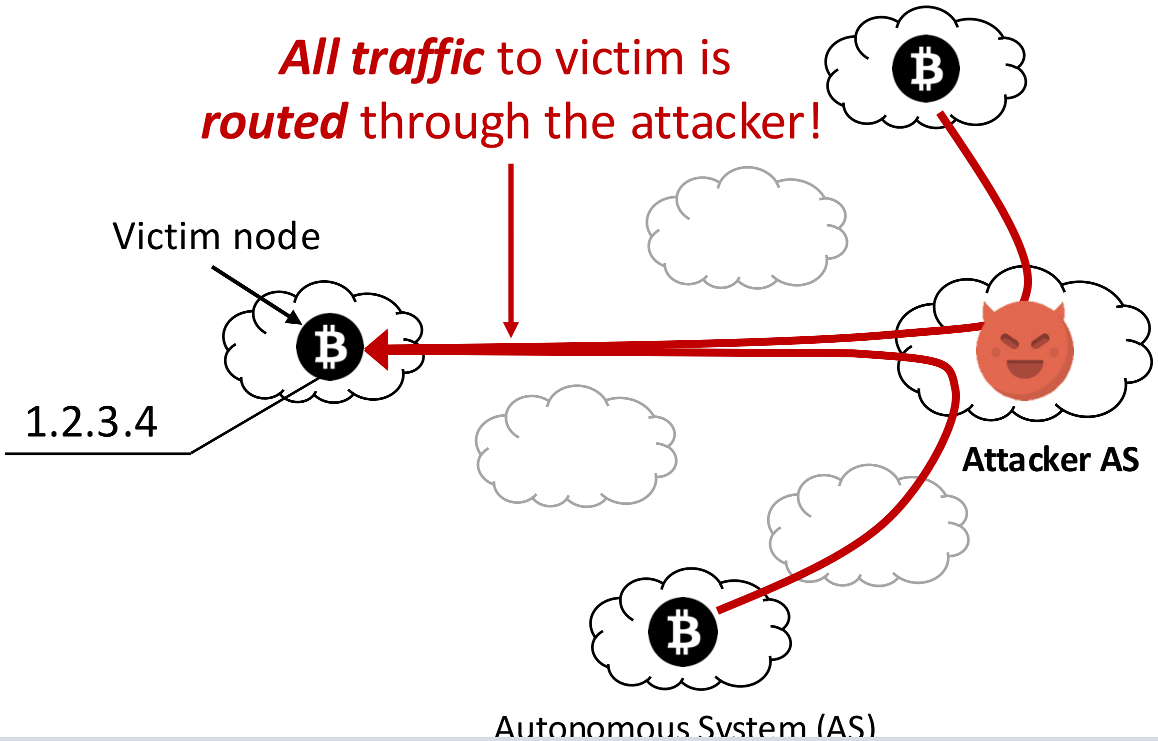
The Canadian Bitcoin Hijack

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

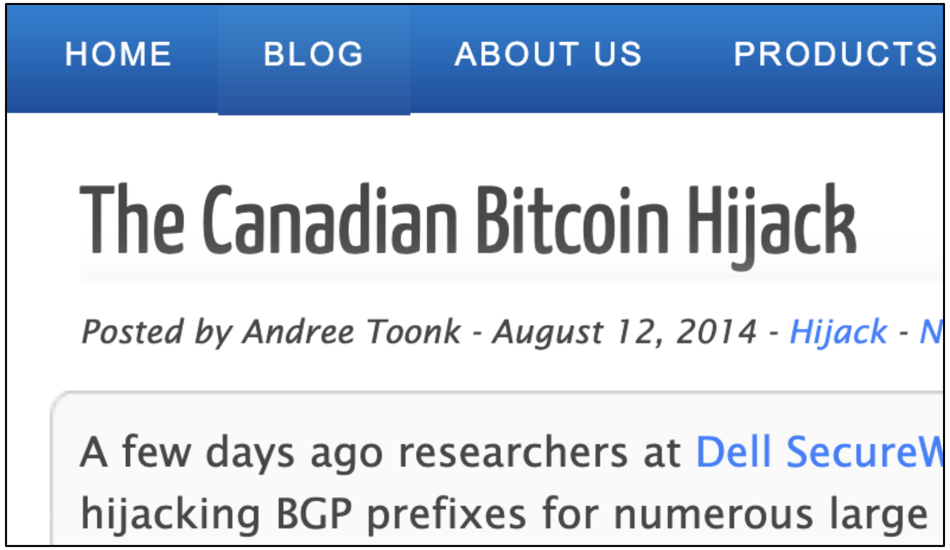
A few days ago researchers at Dell SecureW
hijacking BGP prefixes for numerous large

Only *<u>one</u>* attack instance observed in practice. Why?

Previous attack: ***routing manipulation*** to partition Bitcoin's peer-to-peer network



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



The Canadian Bitcoin Hijack

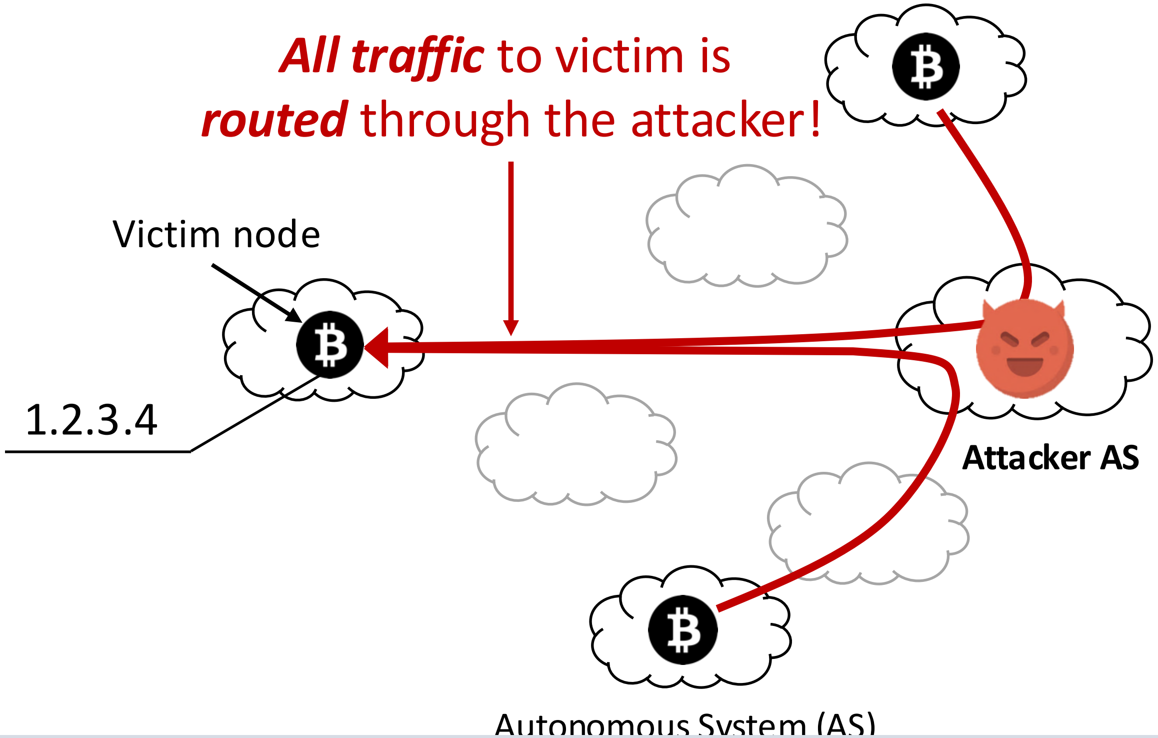
Posted by Andree Toonk - August 12, 2014 - Hijack - N

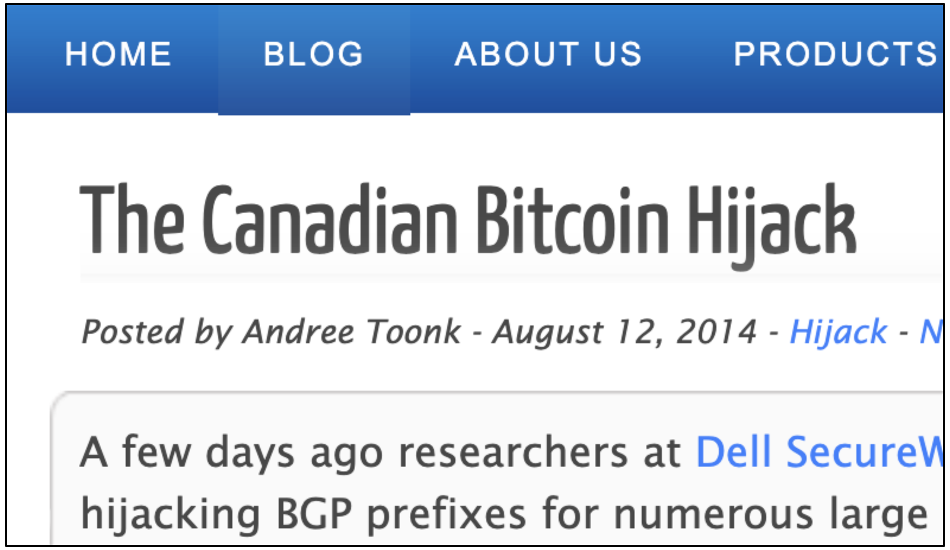
A few days ago researchers at Dell SecureW
hijacking BGP prefixes for numerous large

Only *<u>one</u>* attack instance observed in practice. Why?

- Route manipulation is ***immediately visible*** to the public

Previous attack: ***routing manipulation*** to partition Bitcoin’s peer-to-peer network


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



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?

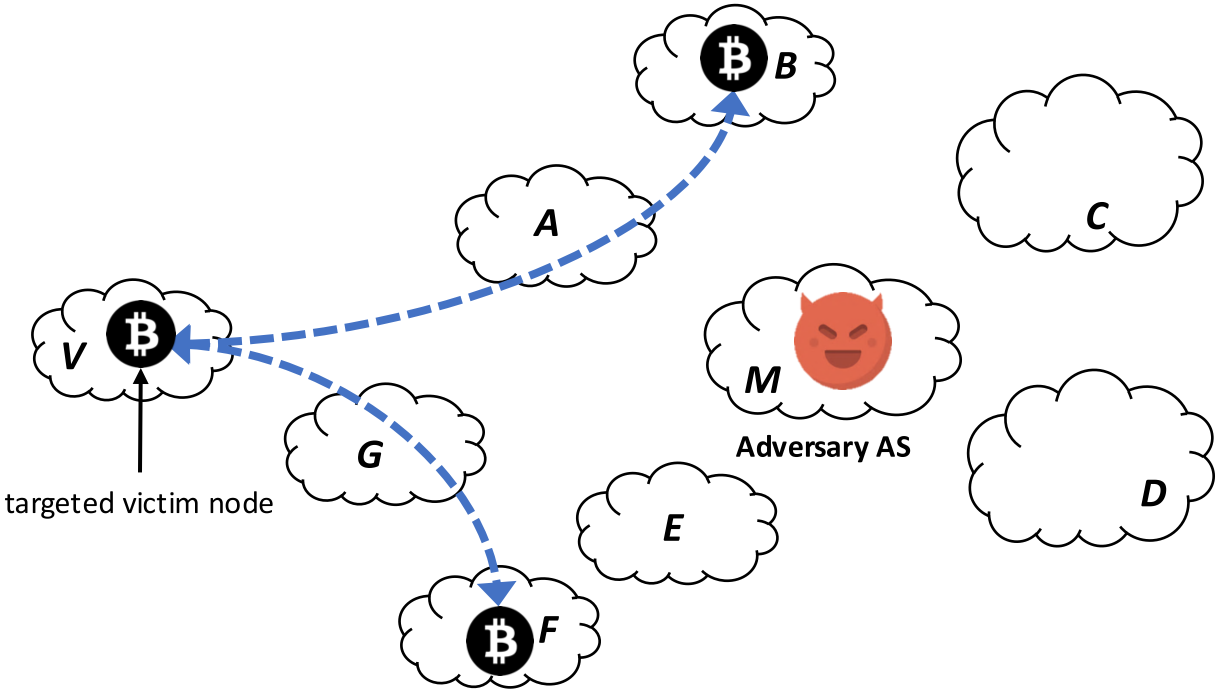
- Route manipulation is ***immediately visible*** to the public
- Attacker’s ***identity*** (AS number) is ***revealed***

Can partitioning attacks be ***stealthier***?

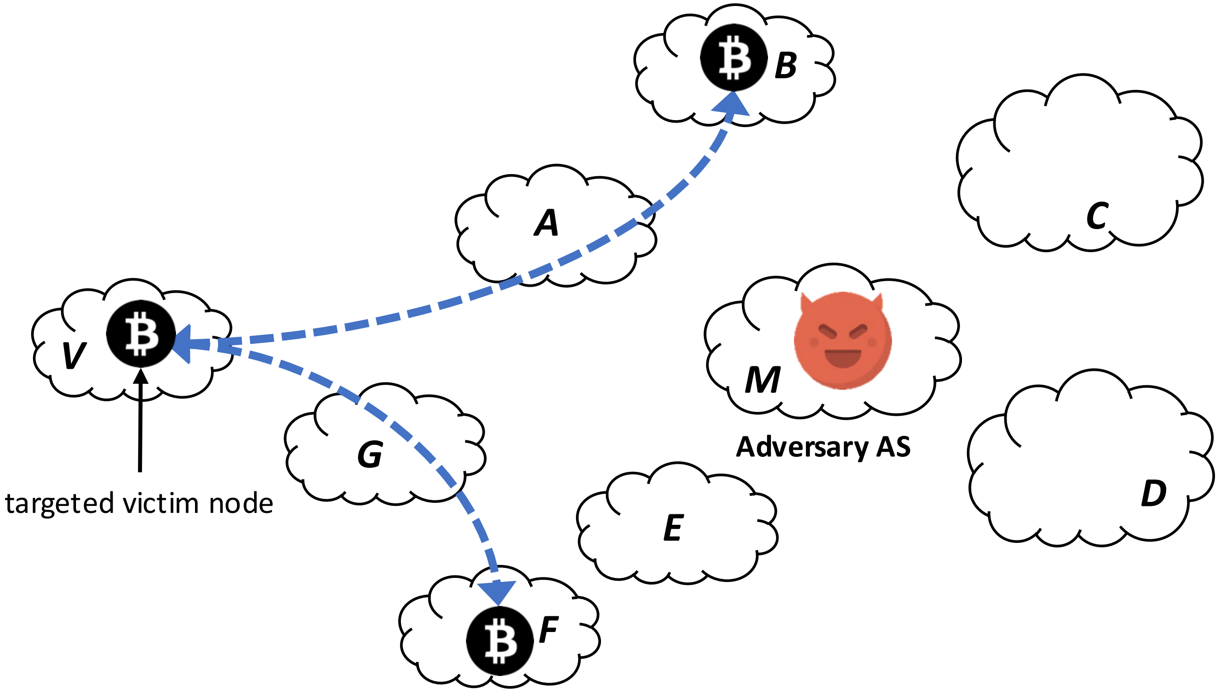
Can partitioning attacks be ***stealthier***?

Erebus attack: A ***stealthier*** partitioning attack against Bitcoin network

Erebus attack: A ***stealthier*** partitioning attack against Bitcoin network

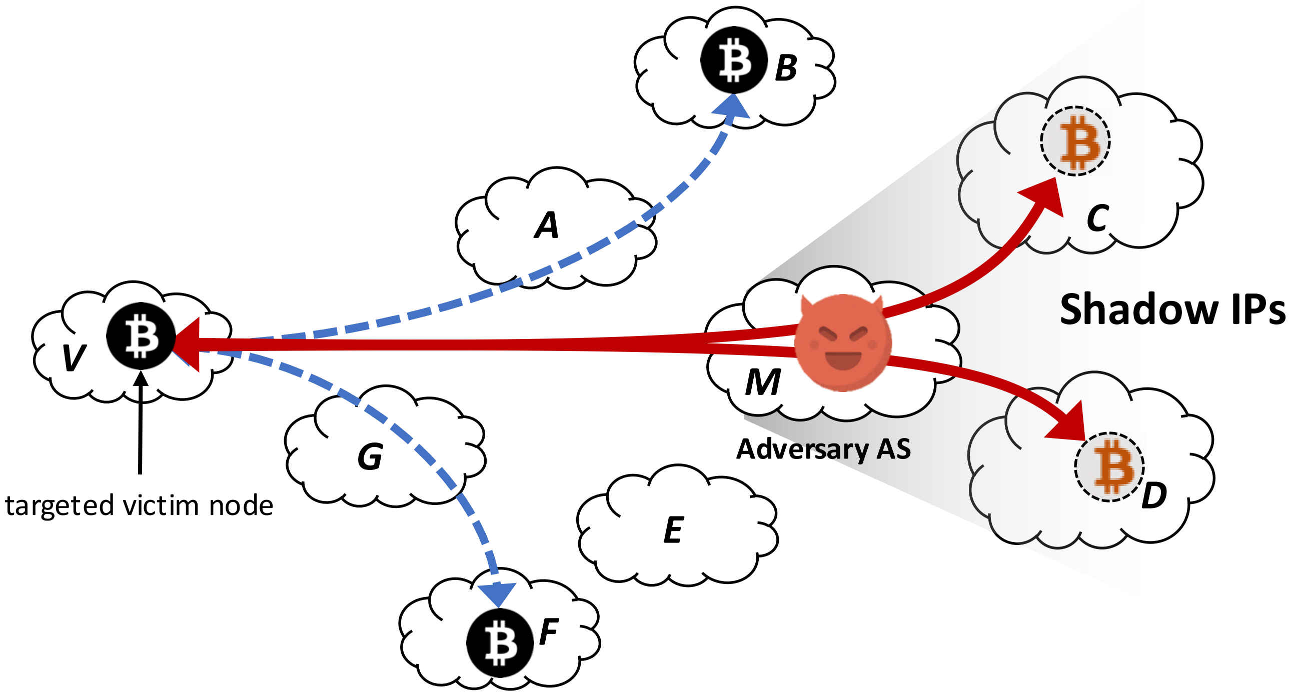


Erebus attack: A ***stealthier*** partitioning attack against Bitcoin network



<u>Idea</u>: ***Indirectly*** force the victim node connects to ***"shadow"*** IPs:

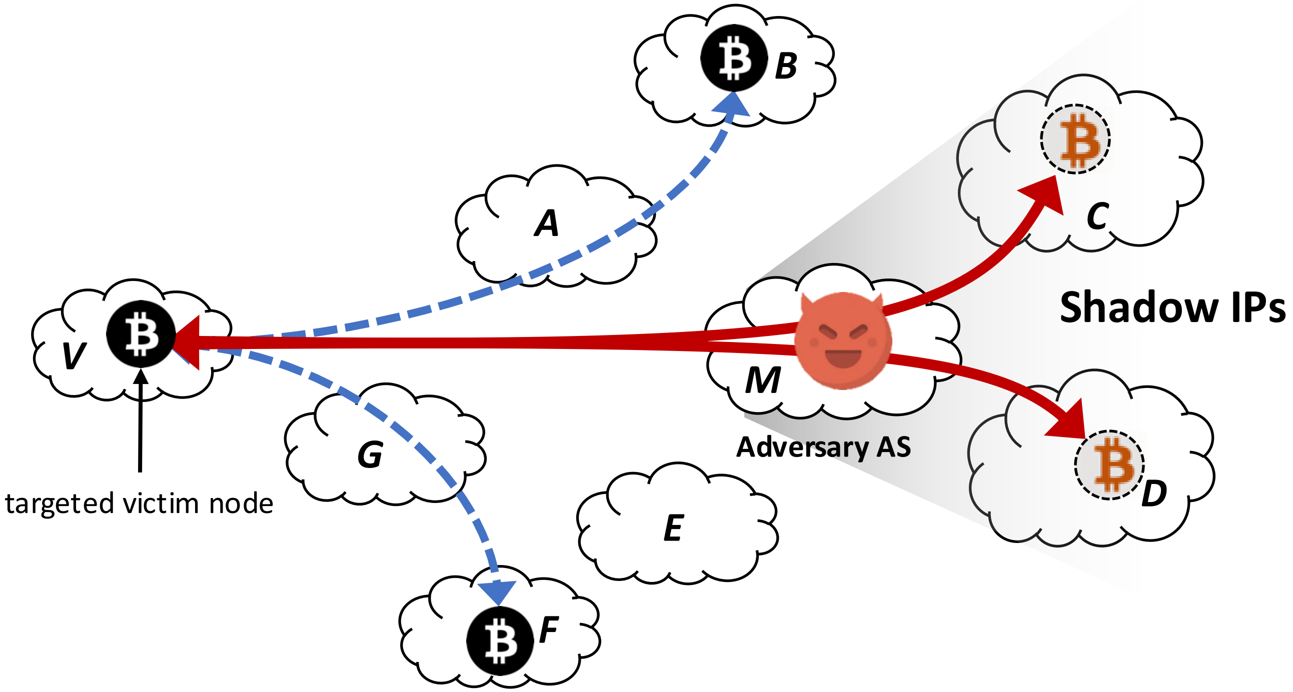
Erebus attack: A ***stealthier*** partitioning attack against Bitcoin network



<u>Idea</u>: ***Indirectly*** force the victim node connects to ***"shadow"*** IPs:

✓ ***Shadow IP*** has the victim-to-itself route includes adversary AS

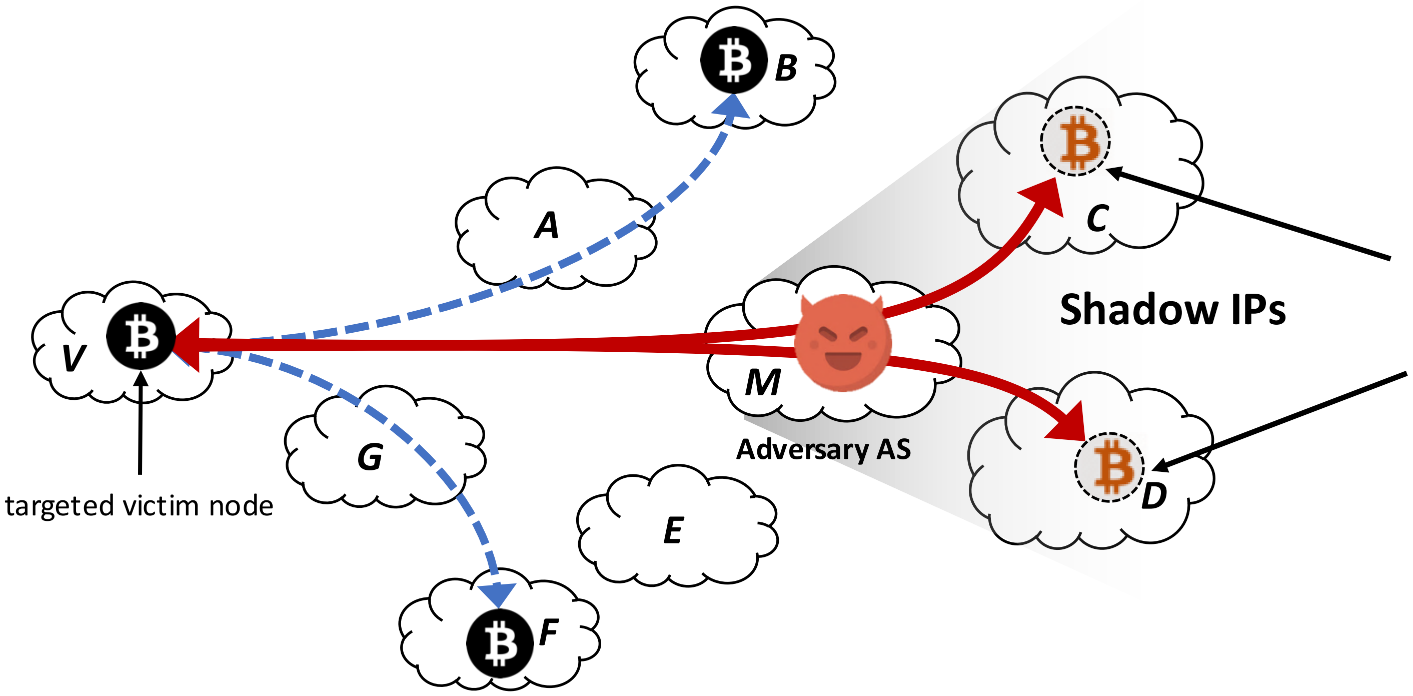
Erebus attack: A ***stealthier*** partitioning attack against Bitcoin network



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!

Erebus attack: A ***stealthier*** partitioning attack against Bitcoin network



Challenge 1:

Is there enough shadow IPs that the attacker can use?

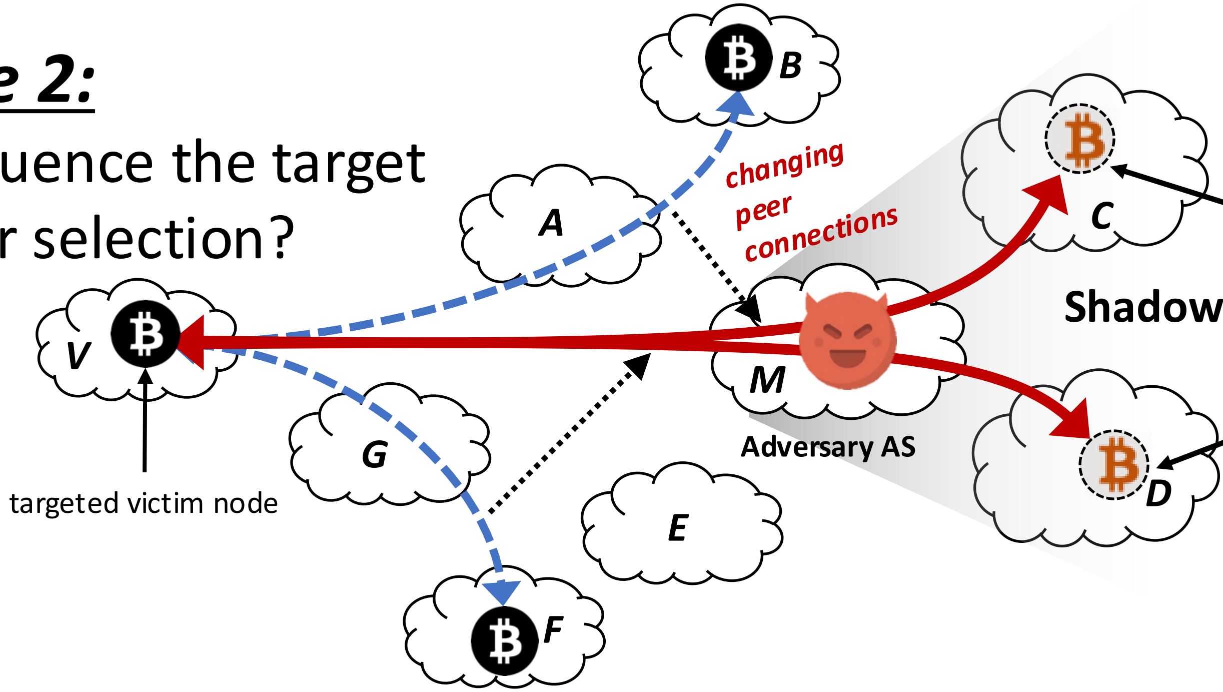
Idea: ***Indirectly*** force the victim node connects to ***"shadow"*** IPs:

- ✓ ***Shadow IP*** has the victim-to-itself route includes adversary AS
- ✓ Attacker AS is the ***man-in-the-middle*** of all peer connections!

Erebus attack: A ***stealthier*** partitioning attack against Bitcoin network

Challenge 2:

How to influence the target node's peer selection?



Challenge 1:

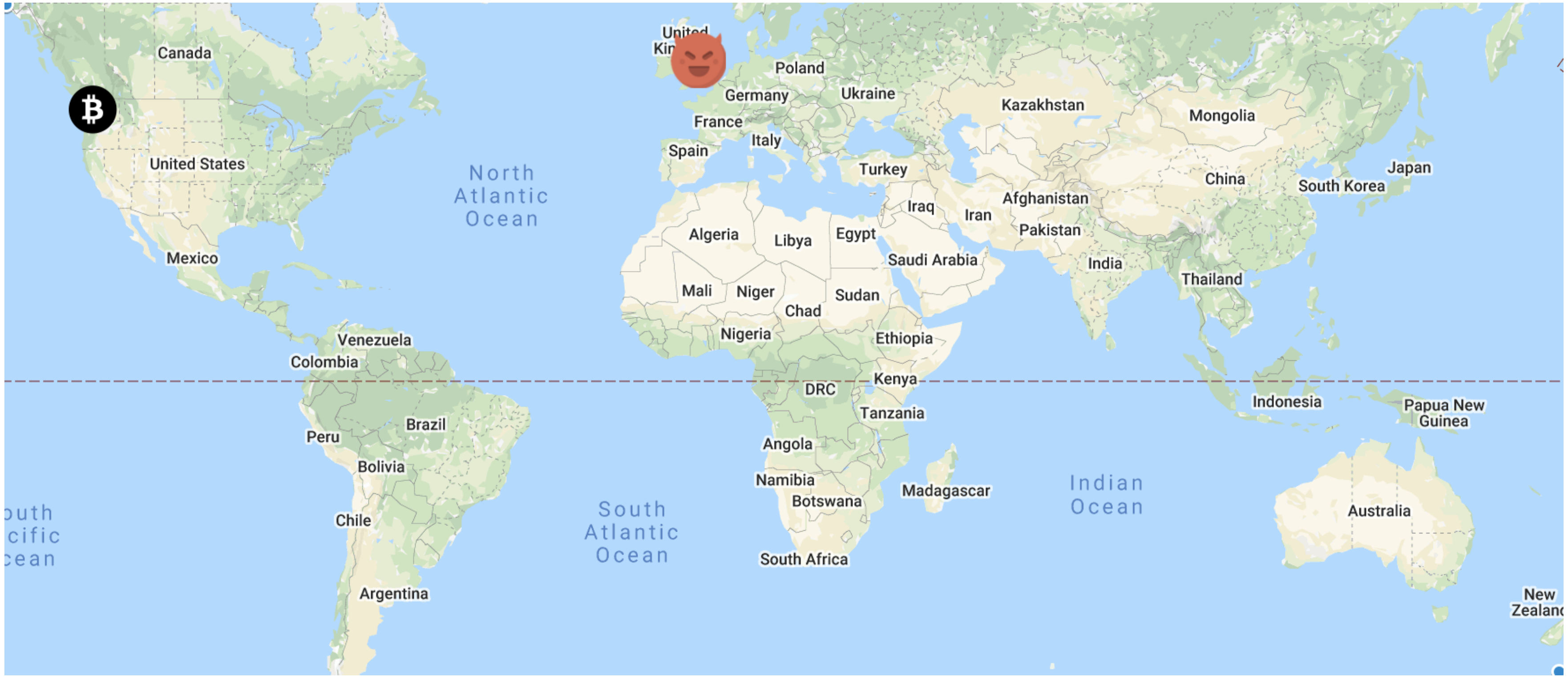
Is there enough shadow IPs that the attacker can use?

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!

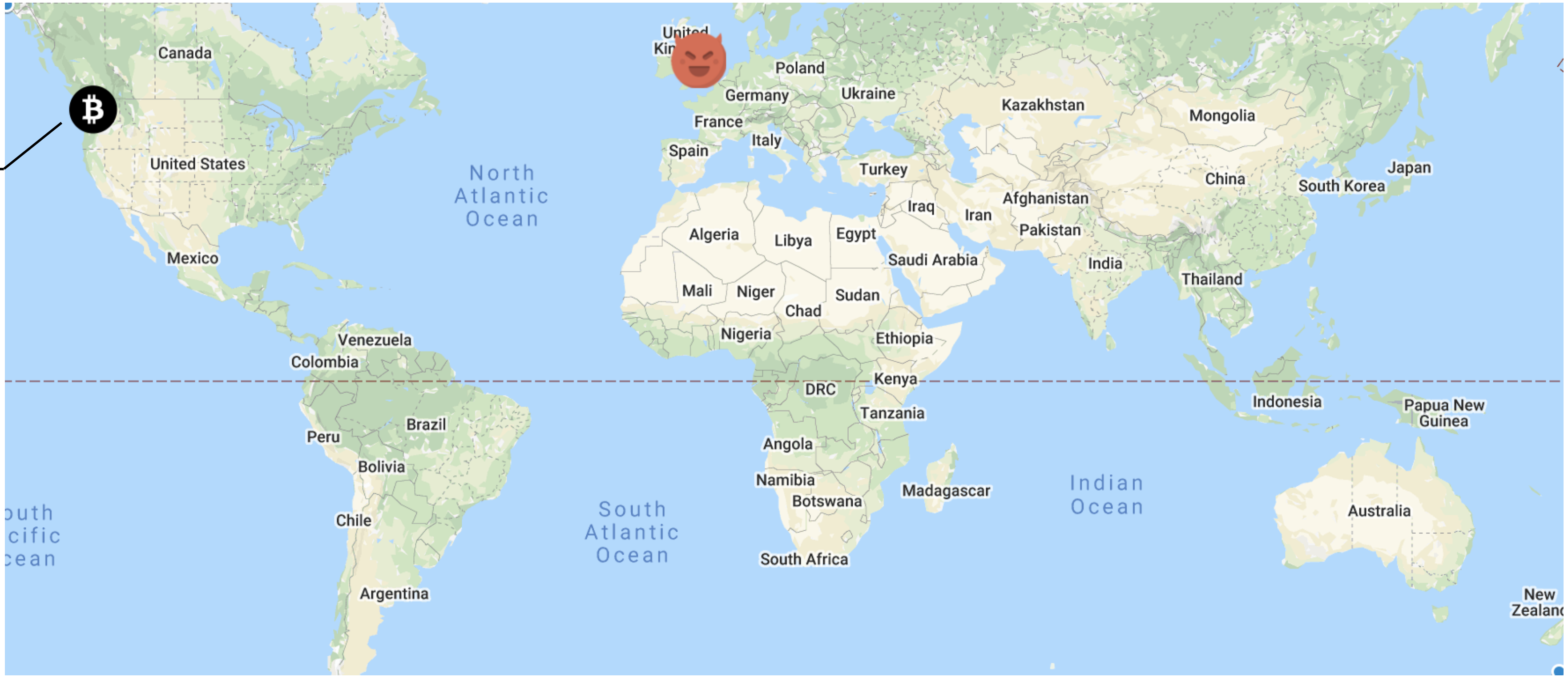
Challenge 1: How many shadow IPs are available?

Challenge 1: How many shadow IPs are available?

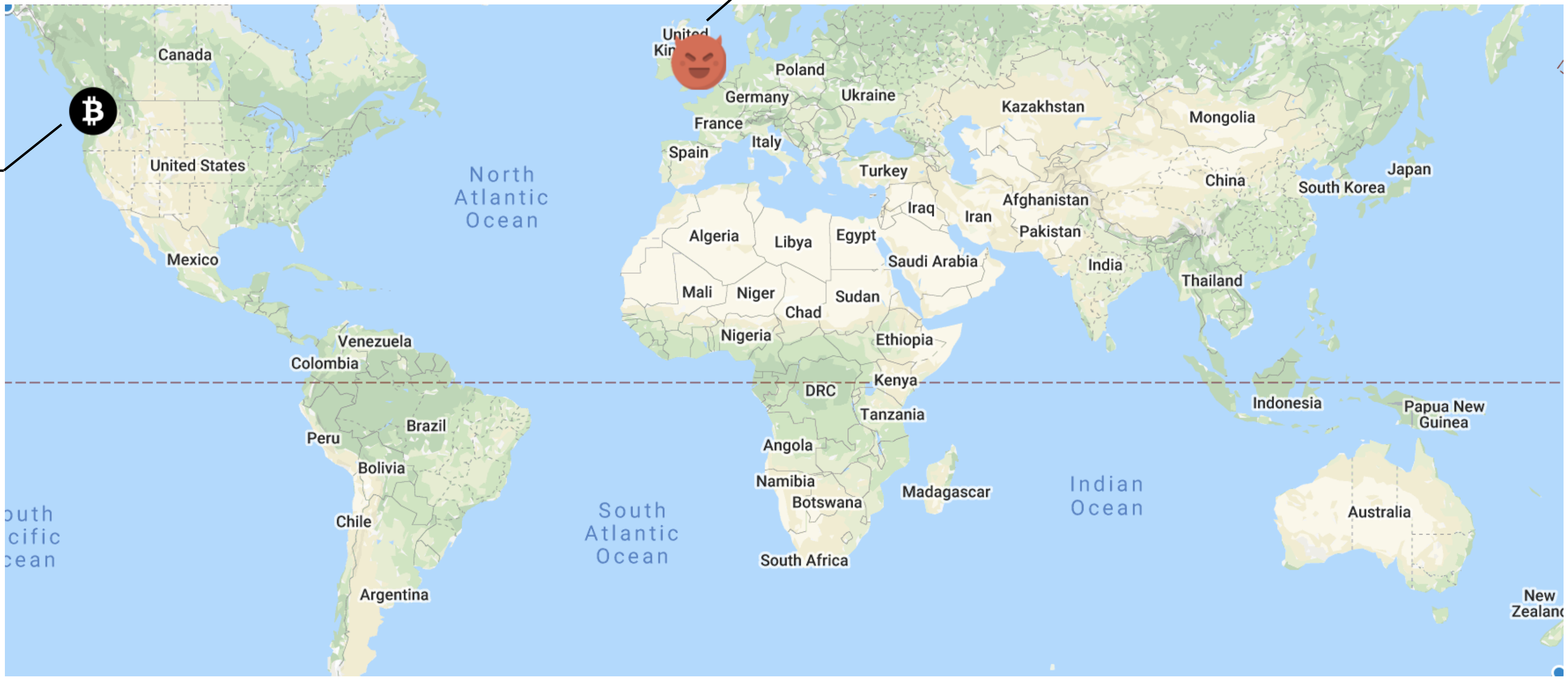


Challenge 1: How many shadow IPs are available?

Victim node (e.g., Amazon)



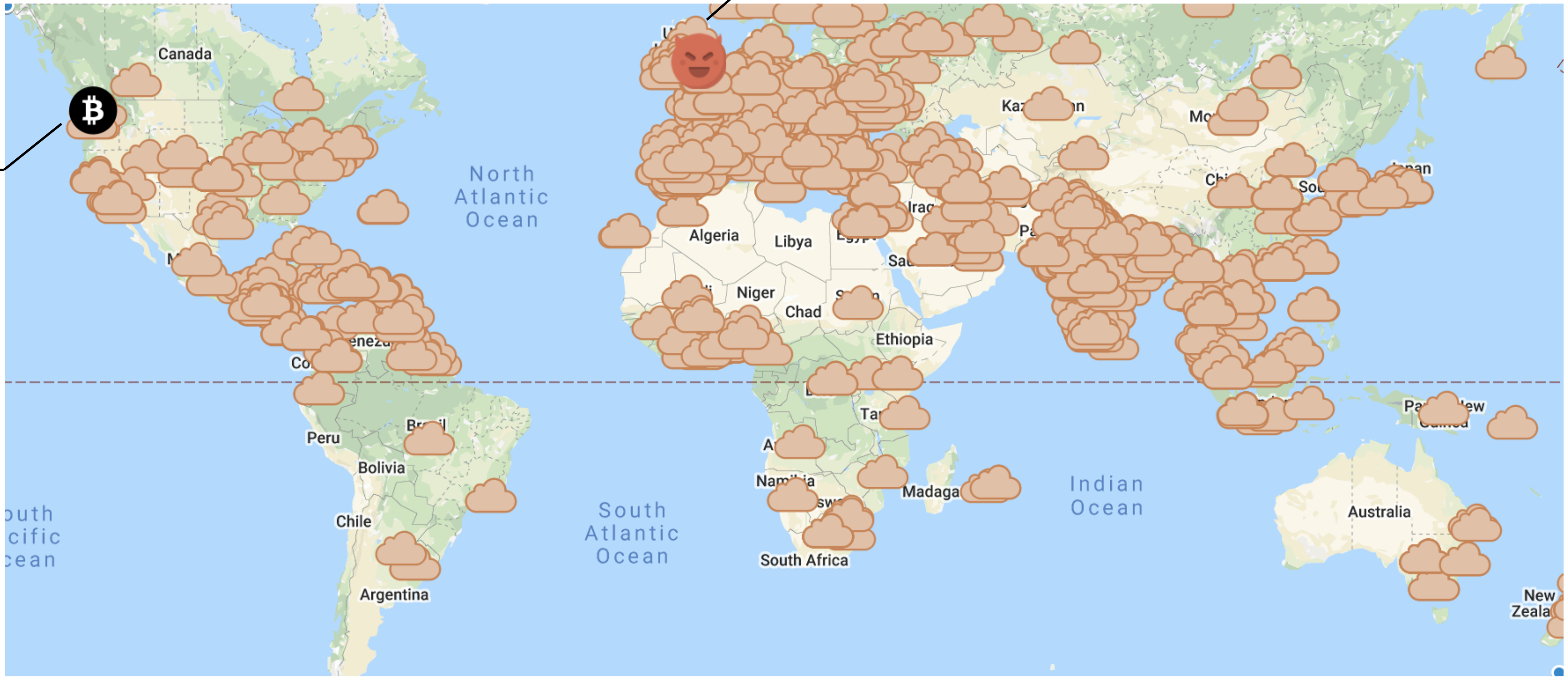
Challenge 1: How many shadow IPs are available?



Victim node (e.g., Amazon)

Attacker AS in Europe

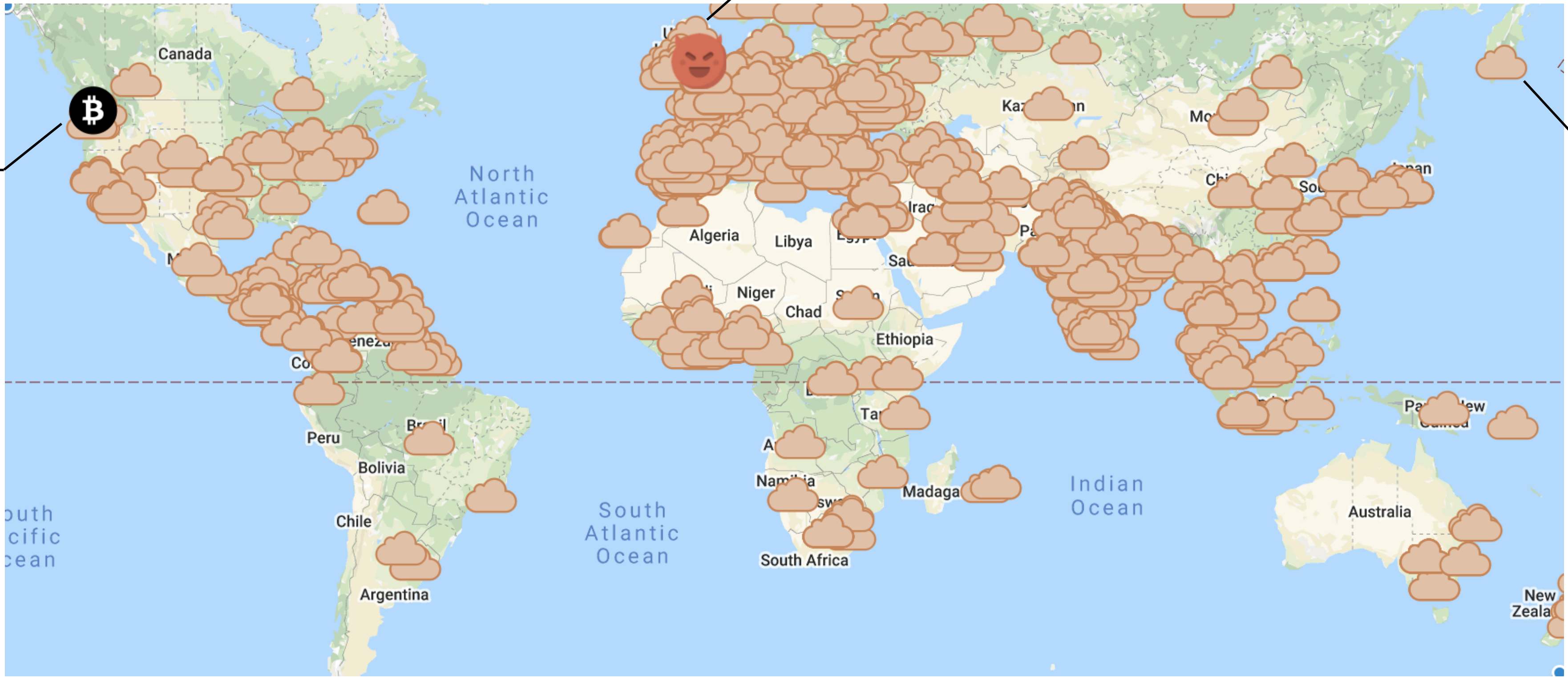
Challenge 1: How many shadow IPs are available?



Attacker AS in Europe

Victim node (e.g., Amazon)

Challenge 1: How many shadow IPs are available?

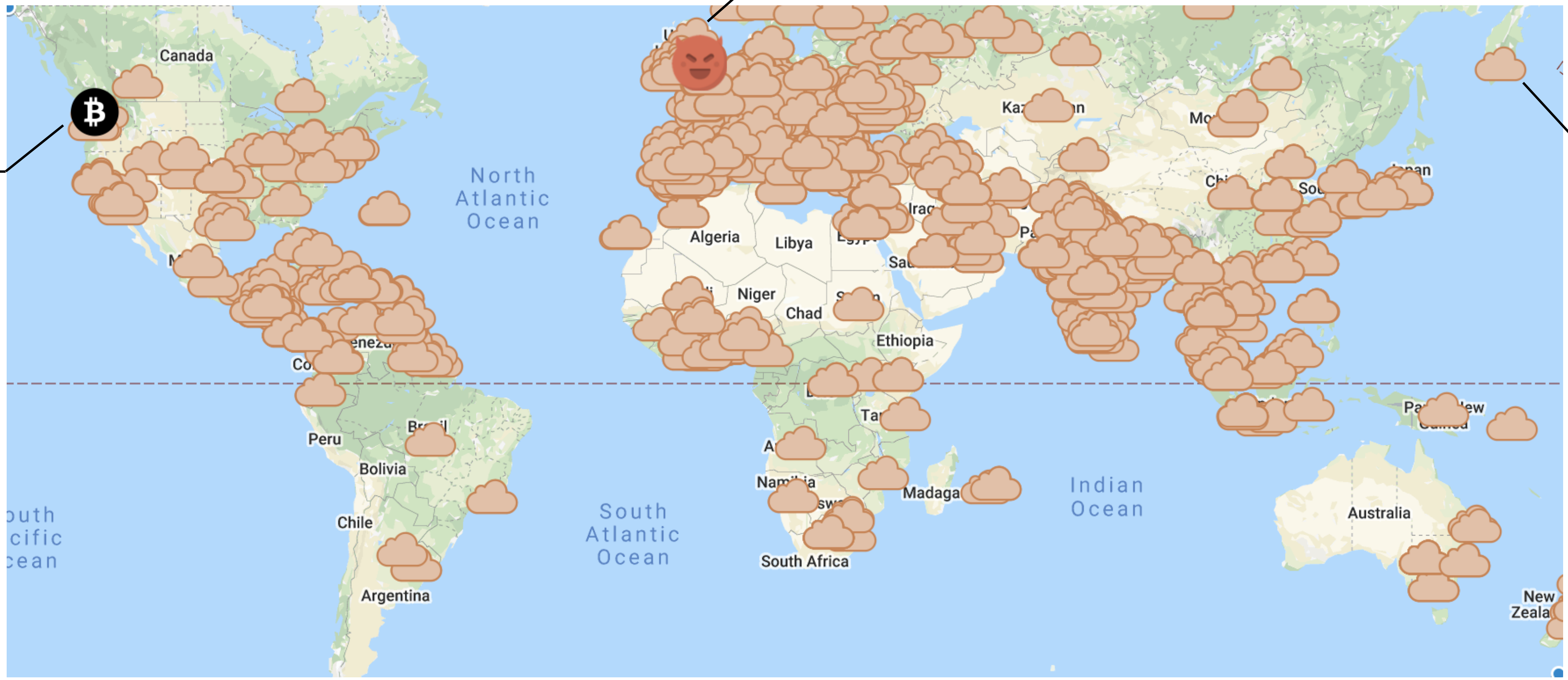


Attacker AS in Europe

Victim node (e.g., Amazon)

Shadow AS

Challenge 1: How many shadow IPs are available?



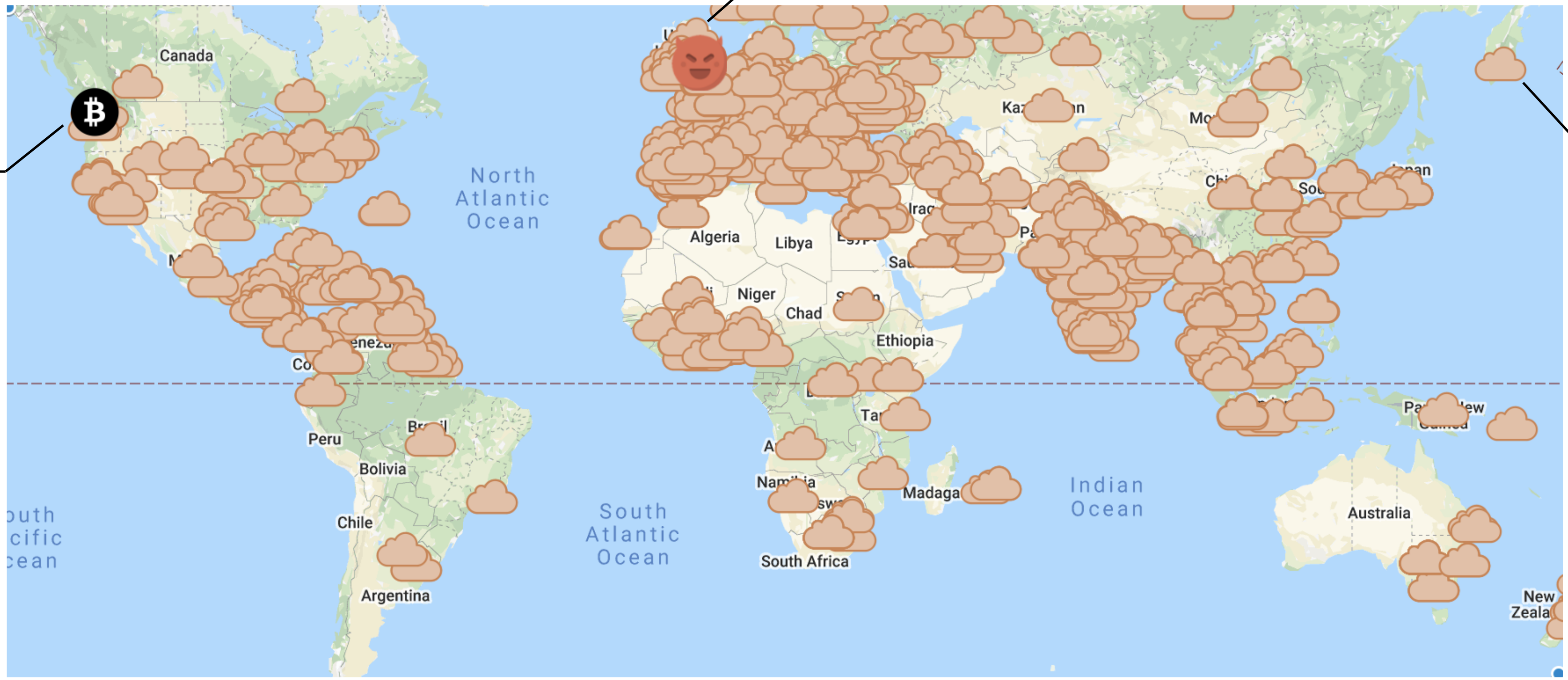
Attacker AS in Europe

Victim node (e.g., Amazon)

Shadow AS

If attacker AS is big enough (e.g., top-100), it can ***easily*** find

Challenge 1: How many shadow IPs are available?



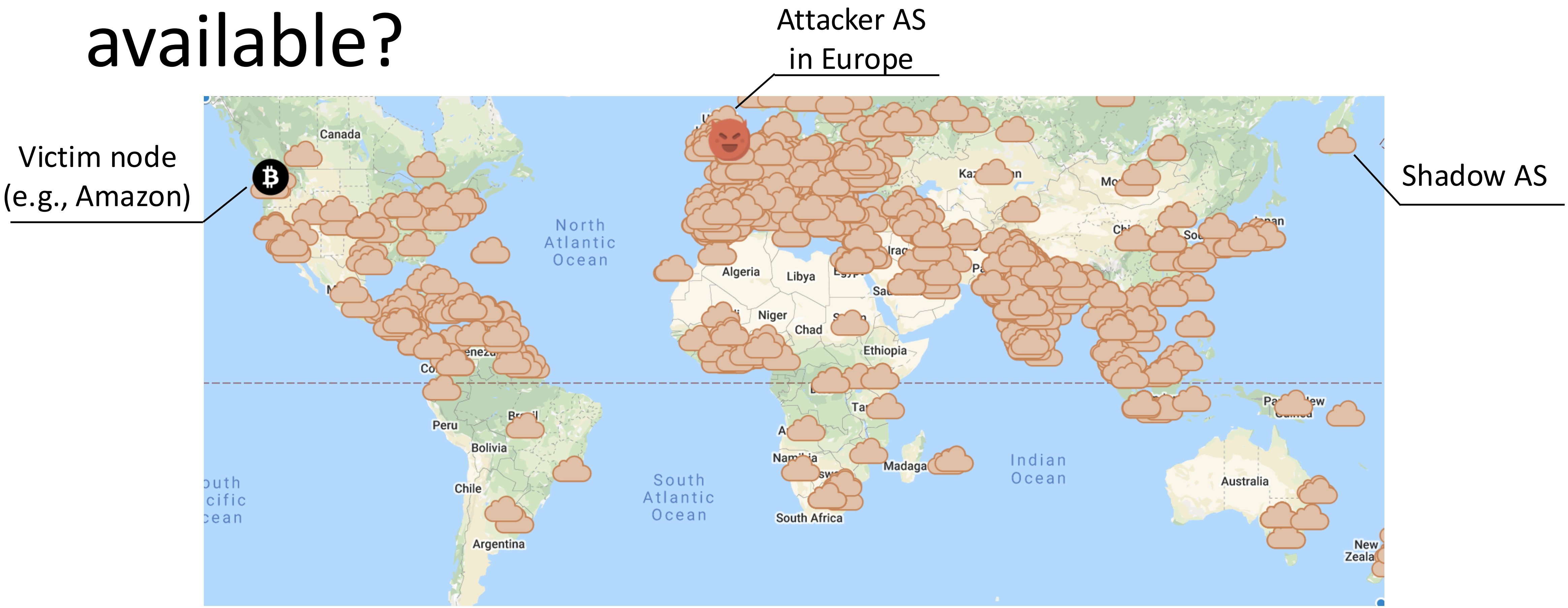
Attacker AS in Europe

Victim node (e.g., Amazon)

Shadow AS

If attacker AS is big enough (e.g., top-100), it can ***easily*** find **hundreds** of shadow ASes

Challenge 1: How many shadow IPs are available?

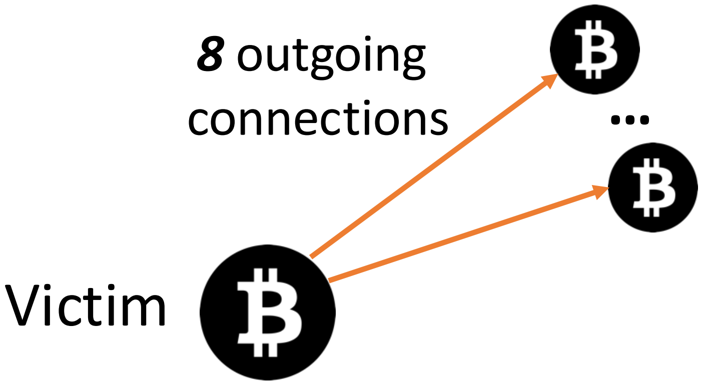


If attacker AS is big enough (e.g., top-100), it can ***easily*** find **hundreds** of shadow ASes => **millions** of shadow IPs

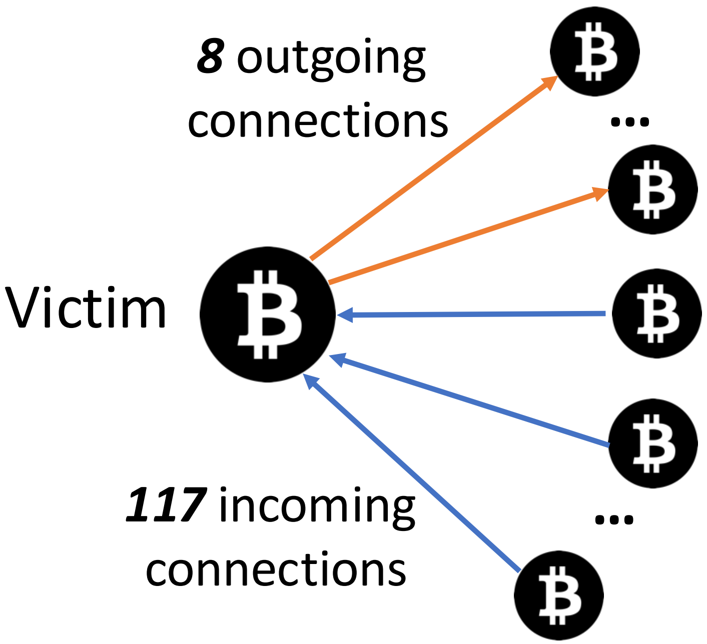
Challenge 2: How does Erebus attacker ***influence*** Bitcoin node’s peer selection?

Victim

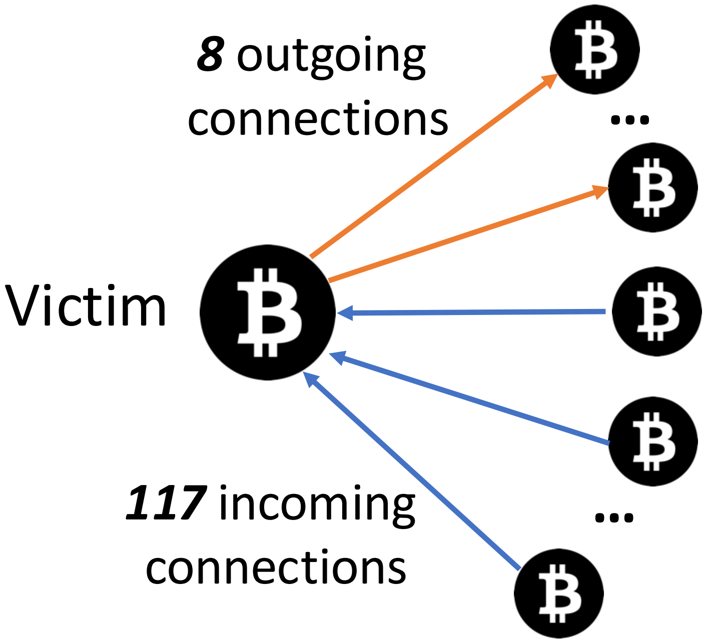
Challenge 2: How does Erebus attacker ***influence*** Bitcoin node's peer selection?

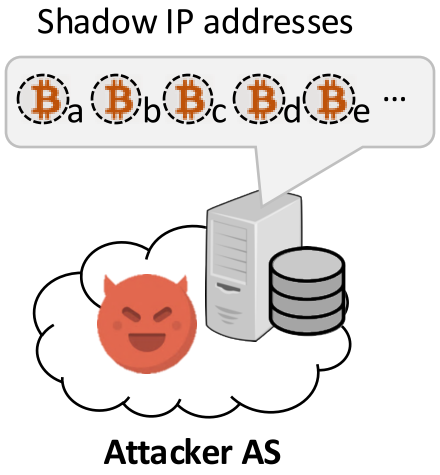


Challenge 2: How does Erebus attacker ***influence*** Bitcoin node's peer selection?

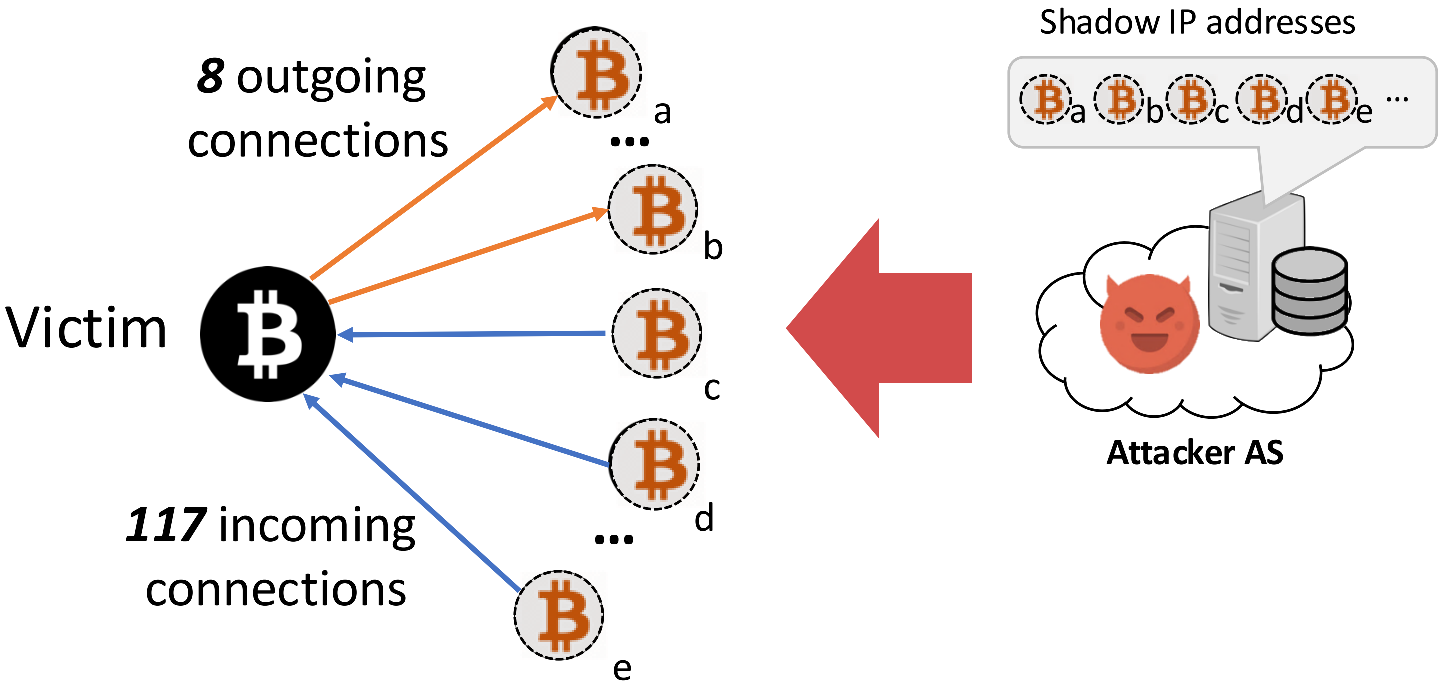


Challenge 2: How does Erebus attacker ***influence*** Bitcoin node's peer selection?

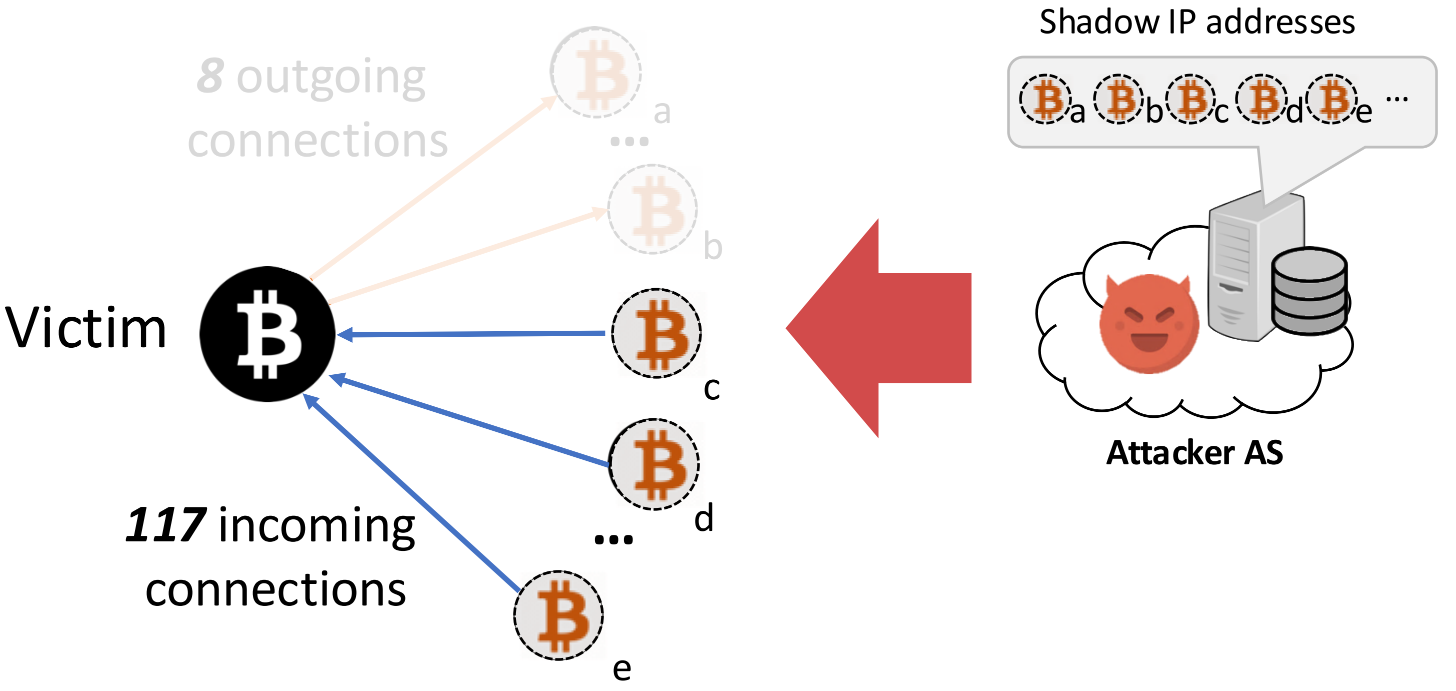




Challenge 2: How does Erebus attacker ***influence*** Bitcoin node's peer selection?

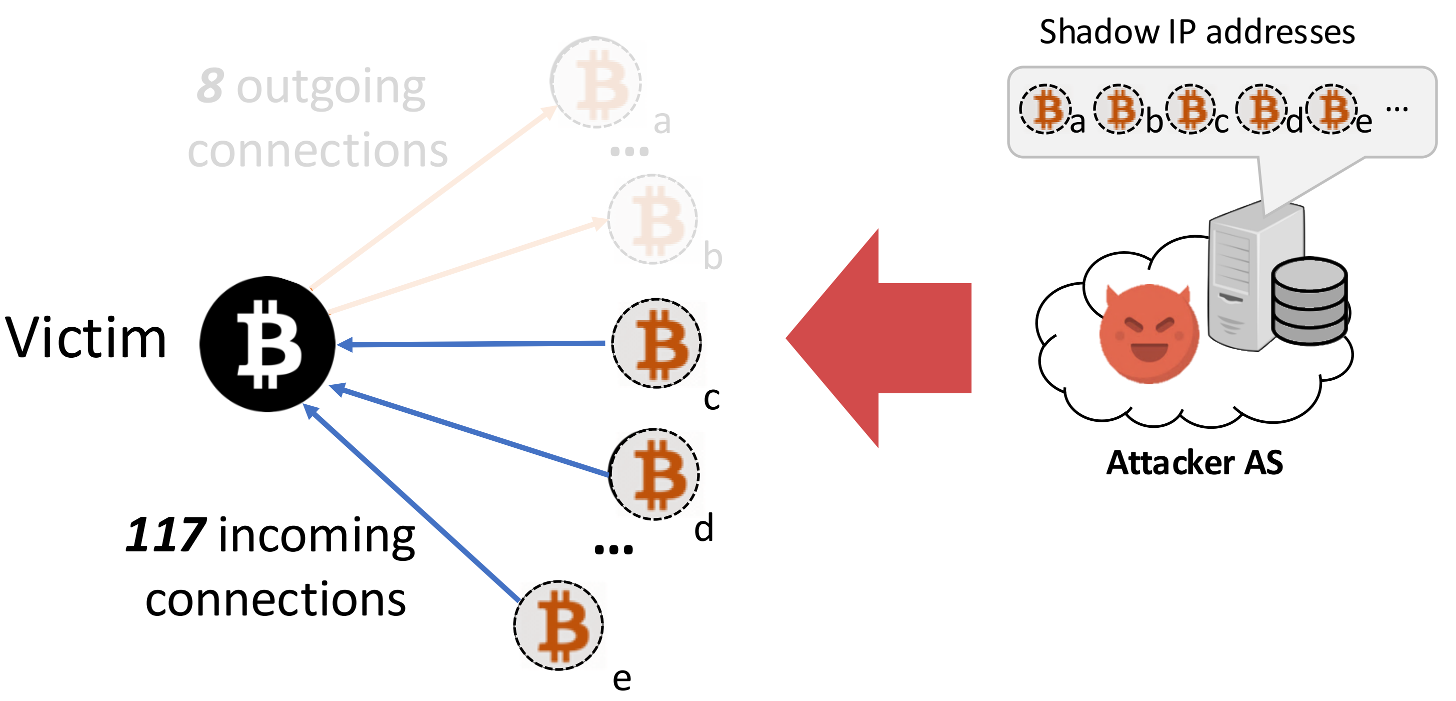


Challenge 2: How does Erebus attacker ***influence*** Bitcoin node's peer selection?



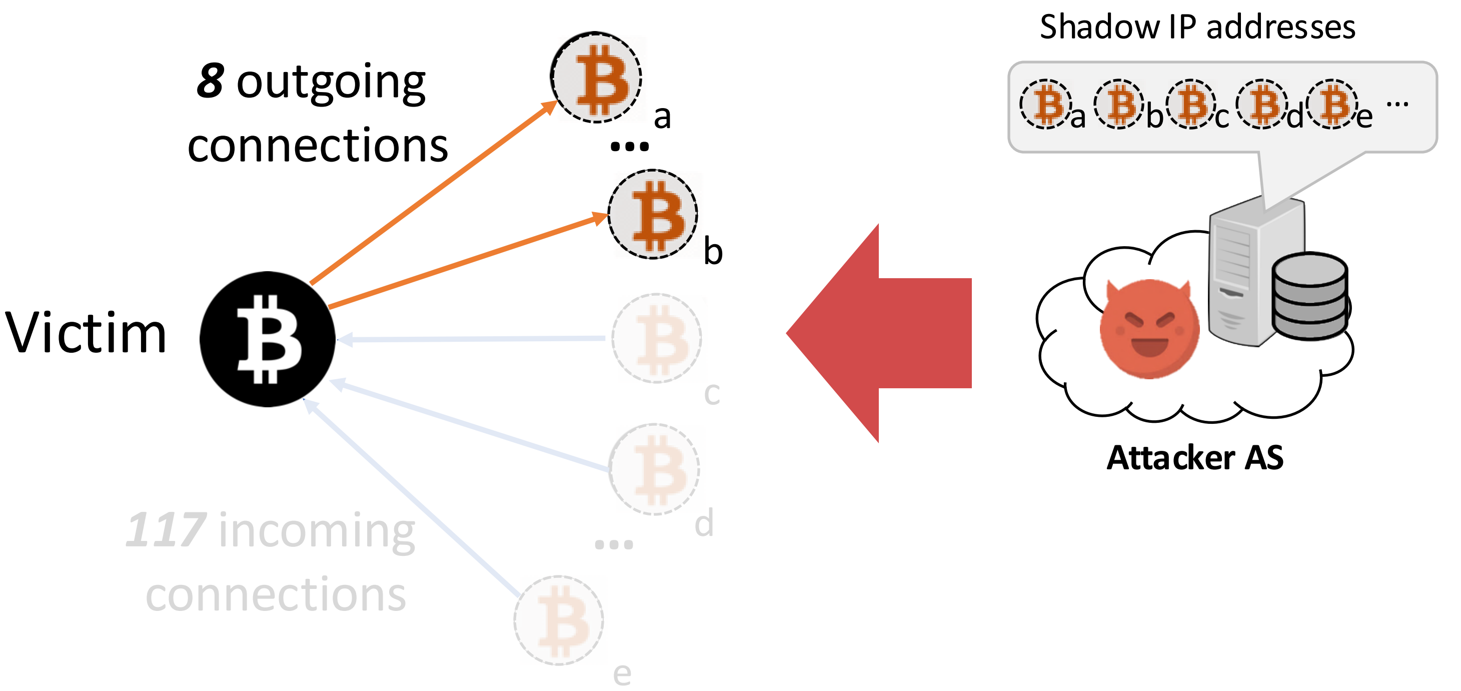
- Occupying 117 incoming connections
  - ✓Connect to the victim ***on behalf*** of the shadow IPs

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

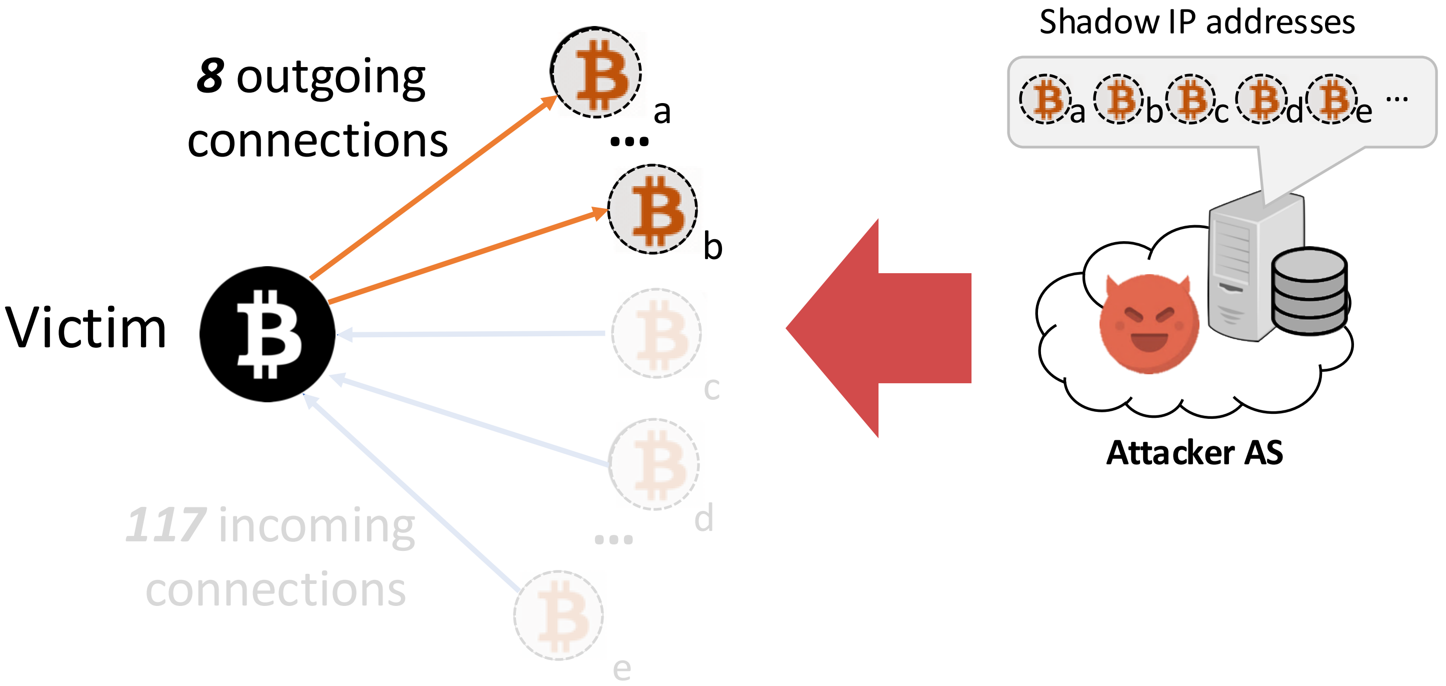
Challenge 2: How does Erebus attacker ***influence*** Bitcoin node's peer selection?



- Occupying 117 incoming connections ***(easier)***
  - ✓Connect to the victim ***on behalf*** of the shadow IPs
- Occupying 8 outgoing connections*
  - ✓Influence the victim to make connections to shadow IPs

(*) 10 outgoing connections since Bitcoin version 0.19.1

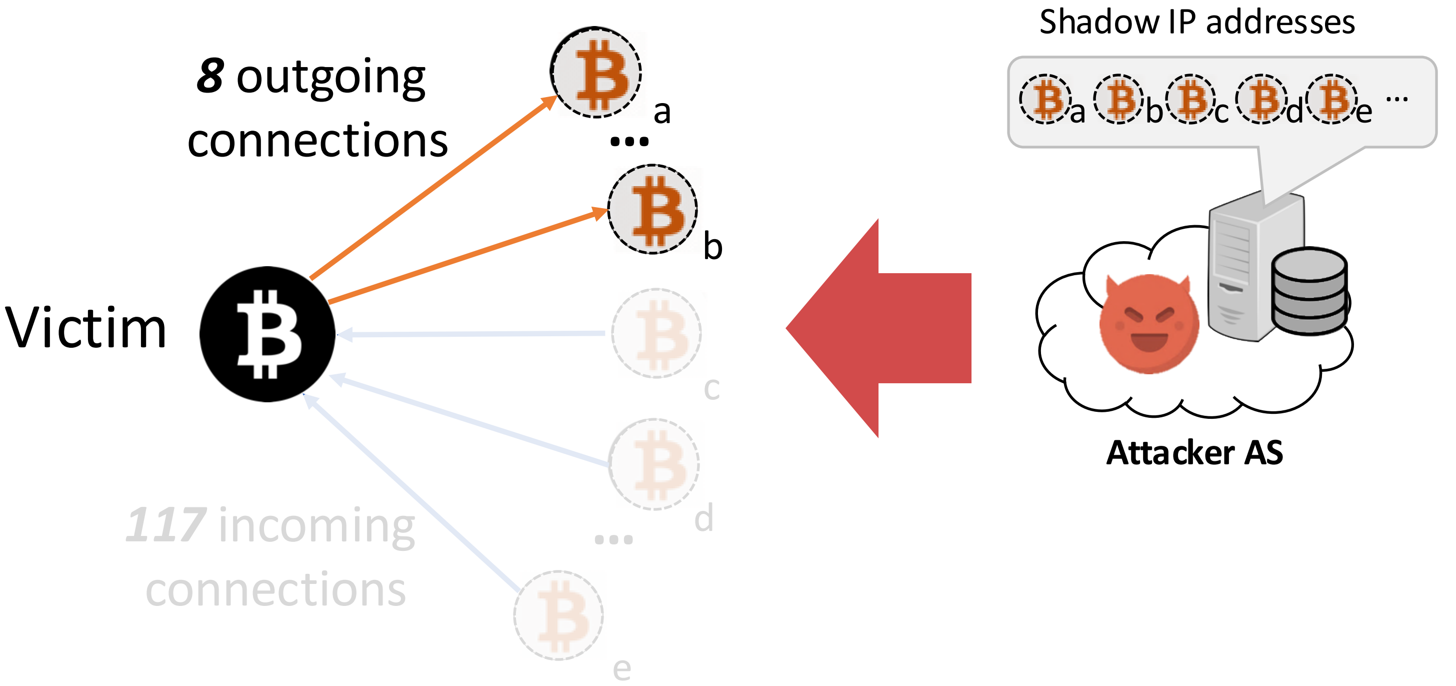
Challenge 2: How does Erebus attacker ***influence*** Bitcoin node's peer selection?



- 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

Challenge 2: How does Erebus attacker ***influence*** Bitcoin node's peer selection?

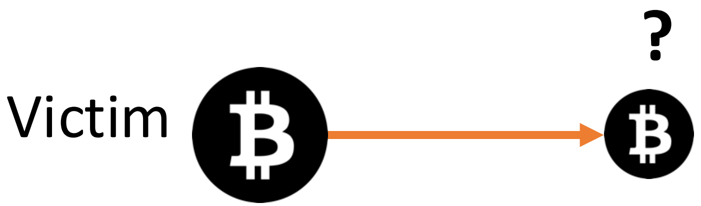


- Occupying 117 incoming connections ***(easier)***
  - ✓Connect to the victim ***on behalf*** of the shadow IPs
- Occupying 8 outgoing connections* ***(much harder!)***
  - ✓Influence the victim to make connections to shadow IPs

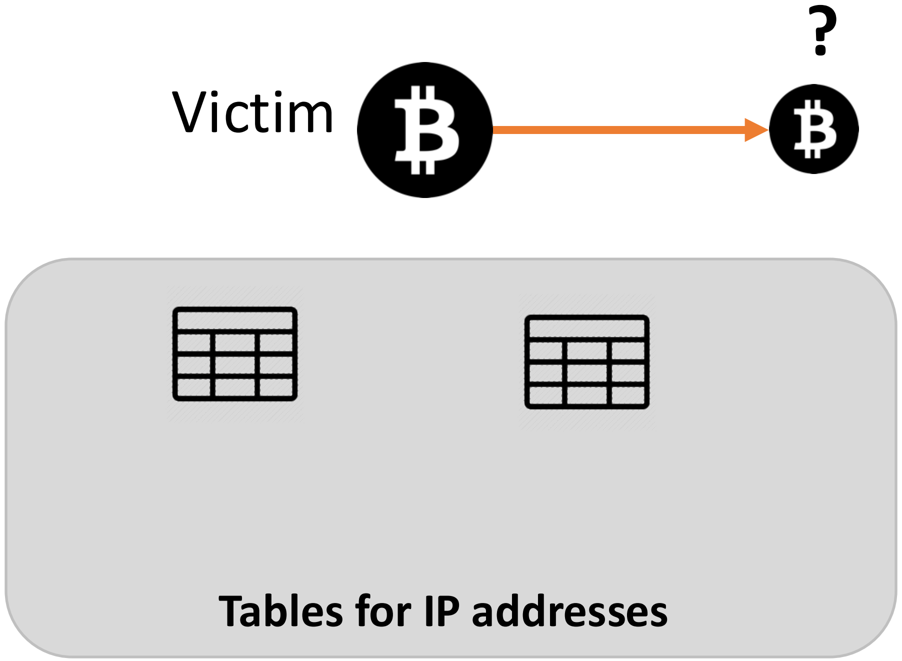
(*) 10 outgoing connections since Bitcoin version 0.19.1

How to ***influence*** the victim to connect to shadow IPs?

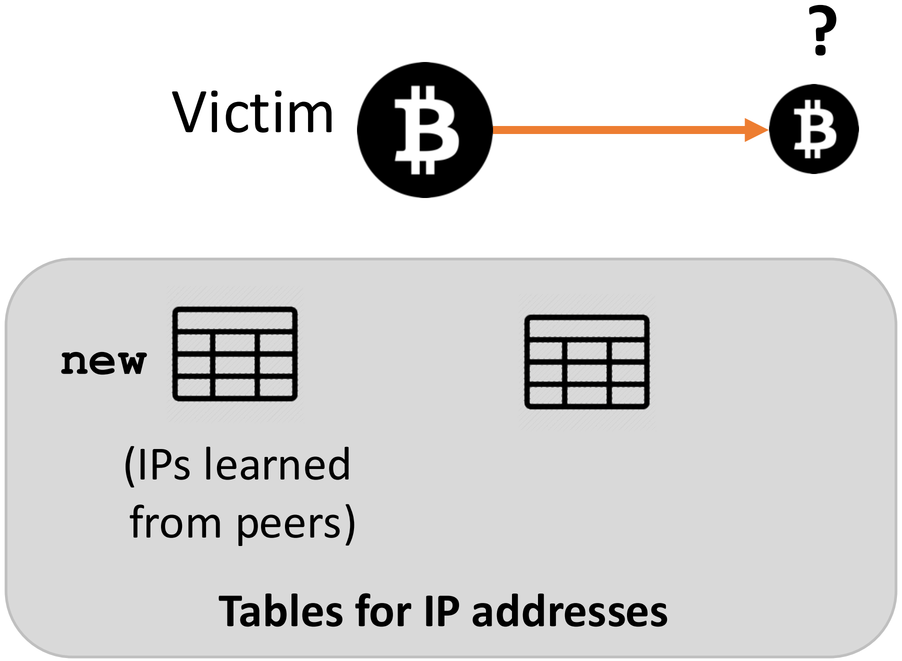
How to ***influence*** the victim to connect to shadow IPs?



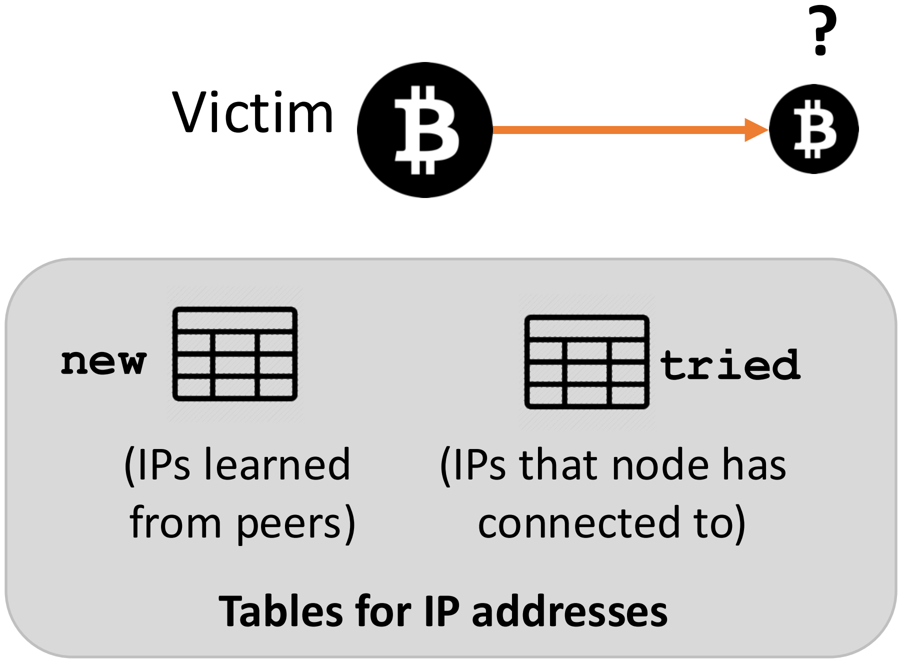
How to ***influence*** the victim to connect to shadow IPs?



How to *influence* the victim to connect to shadow IPs?



How to *influence* the victim to connect to shadow IPs?



Victim

?

new

tried

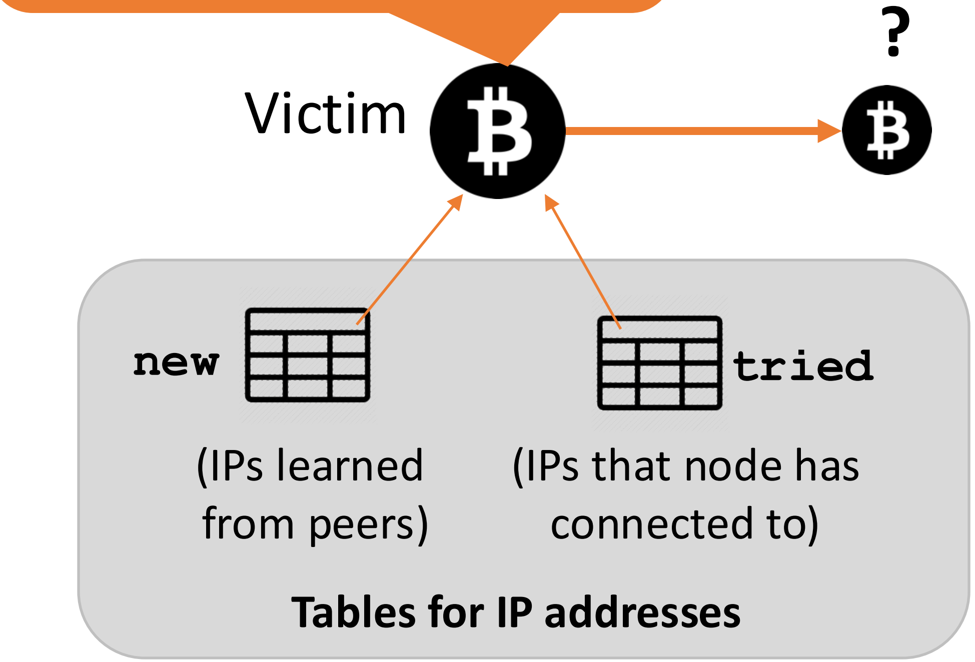
(IPs learned from peers)

(IPs that node has connected to)

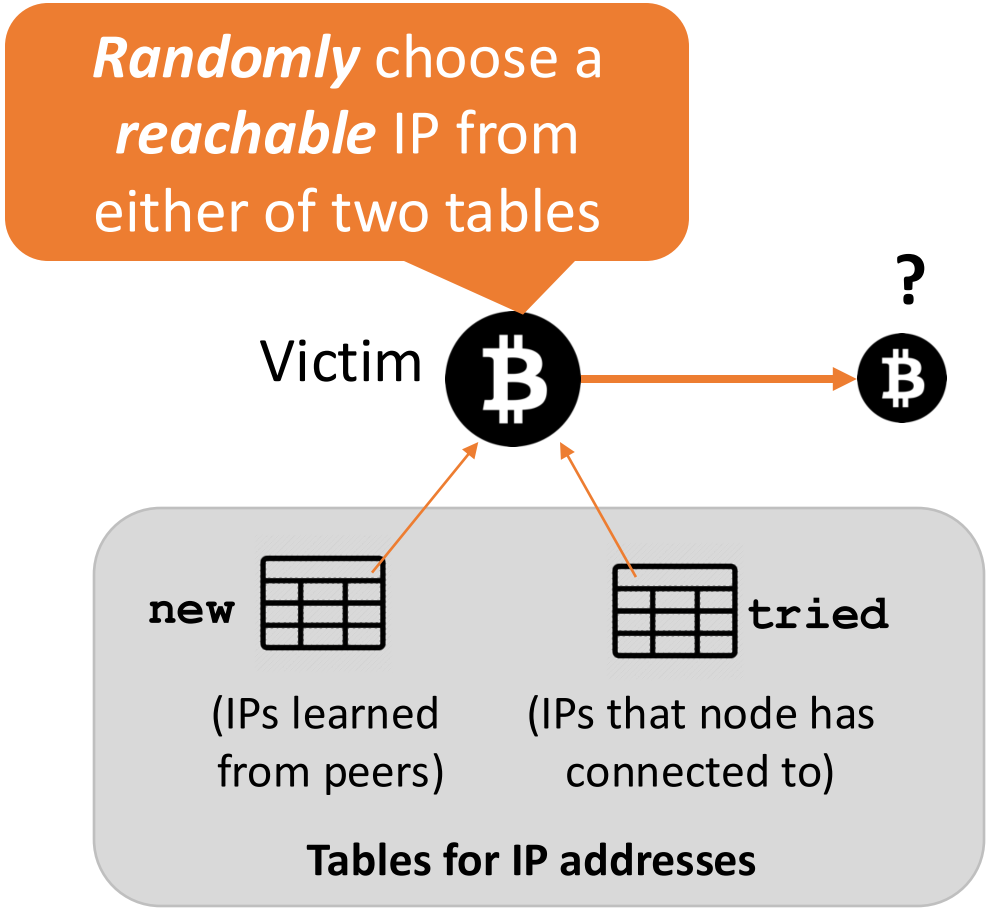
Tables for IP addresses

How to *influence* the victim to connect to shadow IPs?

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

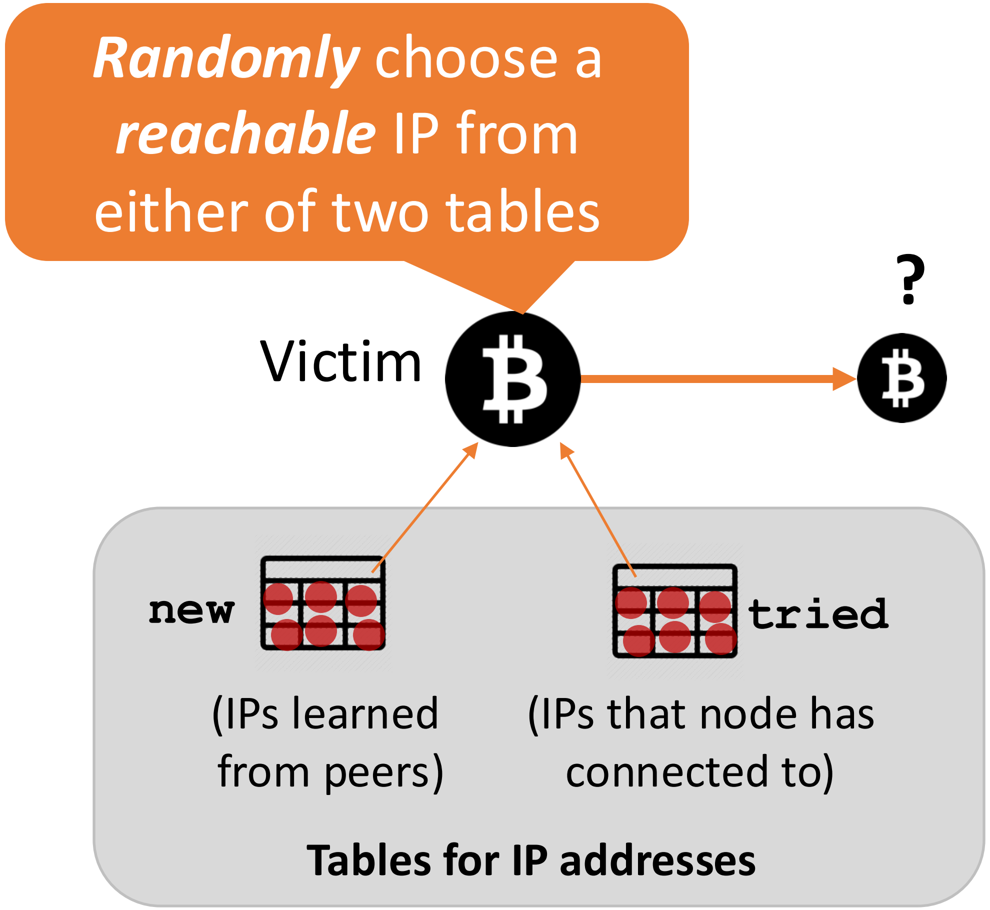


How to *influence* the victim to connect to shadow IPs?


Randomly choose a ***reachable*** IP from either of two tables
?
Victim
new
tried
(IPs learned from peers)
(IPs that node has connected to)
Tables for IP addresses

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

How to *influence* the victim to connect to shadow IPs?



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

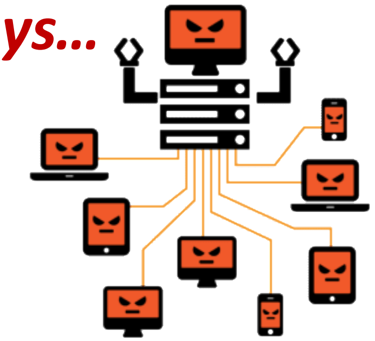
(IPs learned from peers)

(IPs that node has connected to)

Tables for IP addresses

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

In the old days…

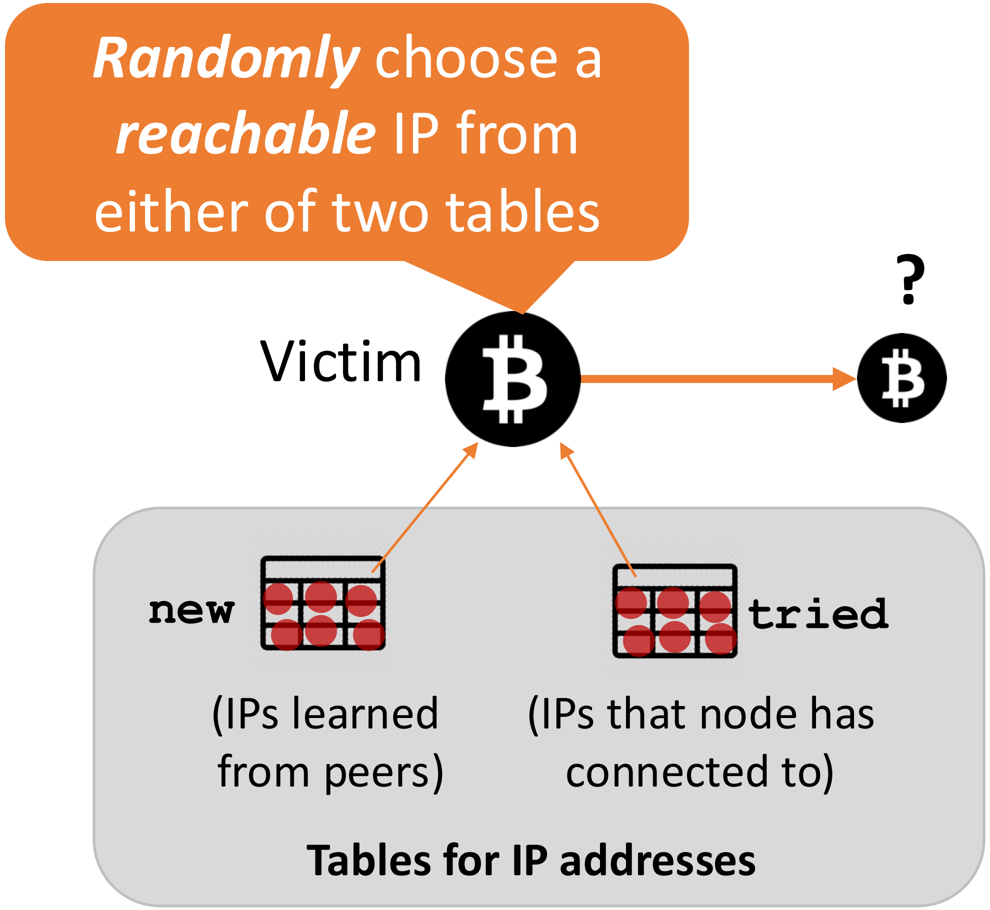


~ 3K bots

Eclipse attack

(Heilman et al., *USENIX Sec'15*)

How to ***influence*** the victim to connect to shadow IPs?



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

(IPs learned from peers)

(IPs that node has connected to)

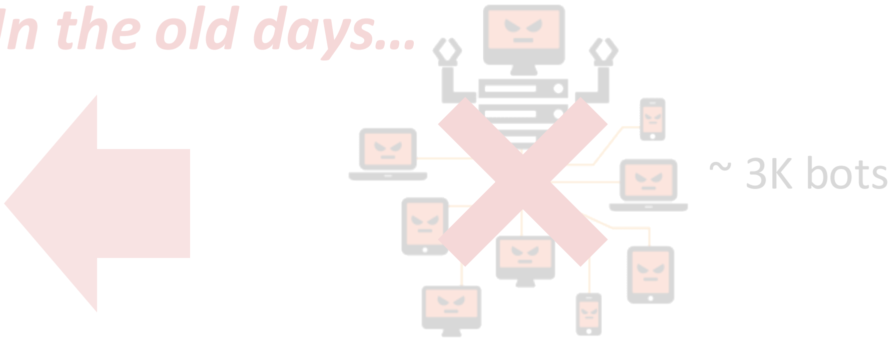
Tables for IP addresses

<u>Our goal</u>: Dominate ***reachable*** IPs in two tables with shadow IPs

<u>Challenges</u>:

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

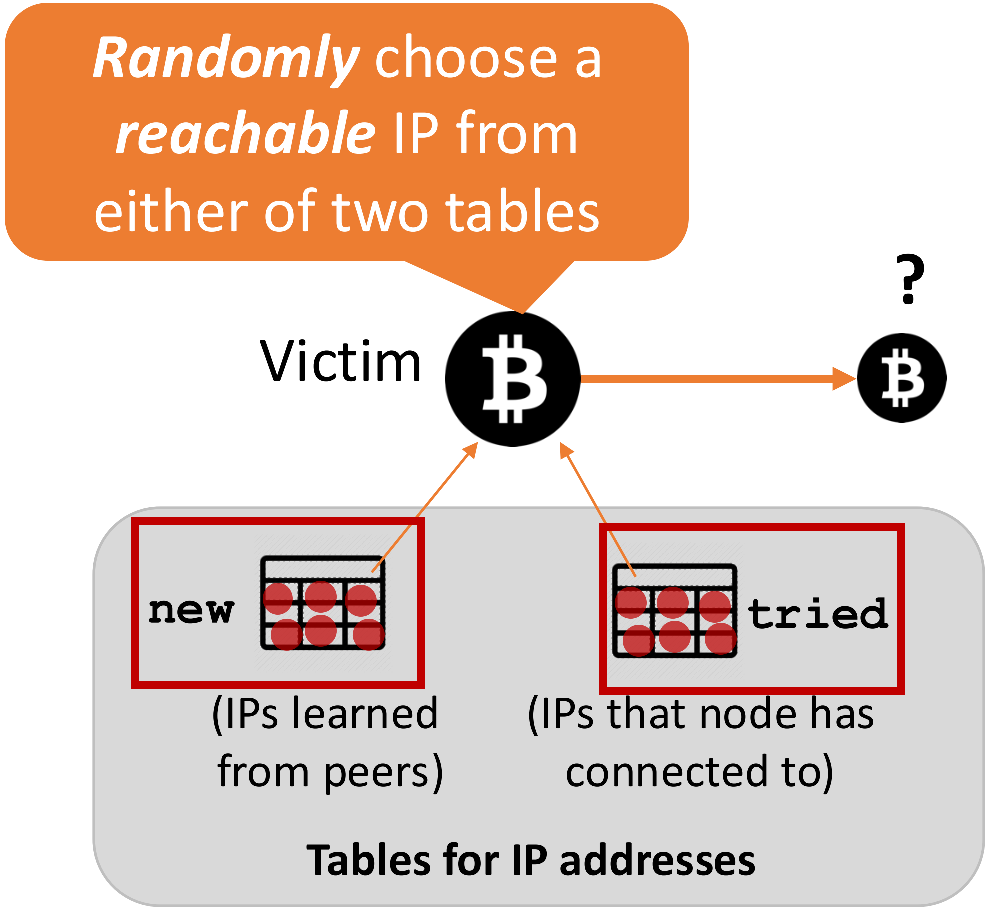
In the old days…



Eclipse attack

(Heilman et al., *USENIX Sec'15*)

How to ***influence*** the victim to connect to shadow IPs?



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

Victim

?

new

tried

(IPs learned from peers)

(IPs that node has connected to)

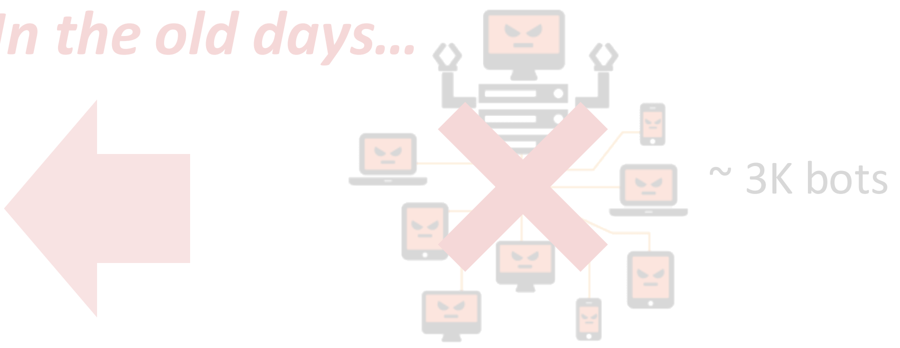
Tables for IP addresses

<u>Our goal</u>: Dominate ***reachable*** IPs in two tables with shadow IPs

<u>Challenges</u>:

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

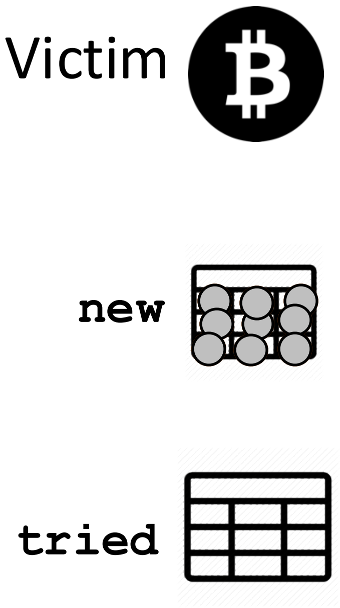
In the old days…



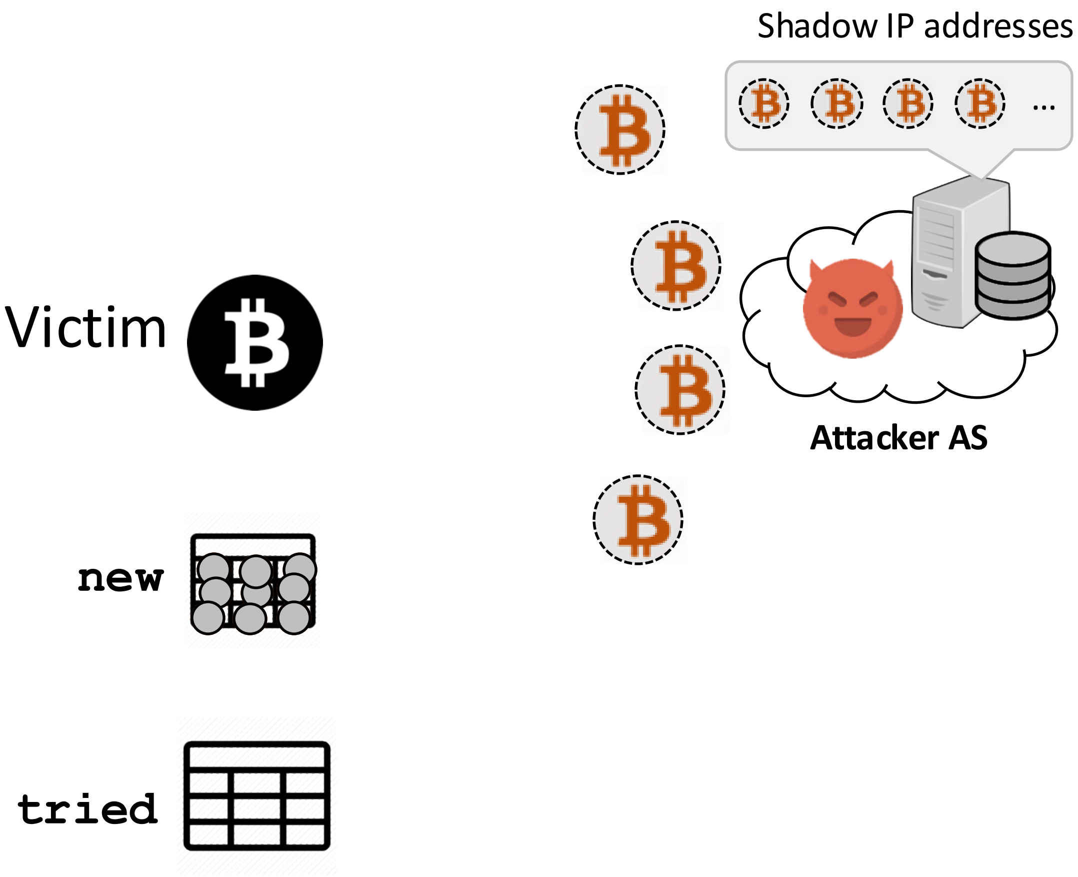
Eclipse attack

(Heilman et al., *USENIX Sec'15*)

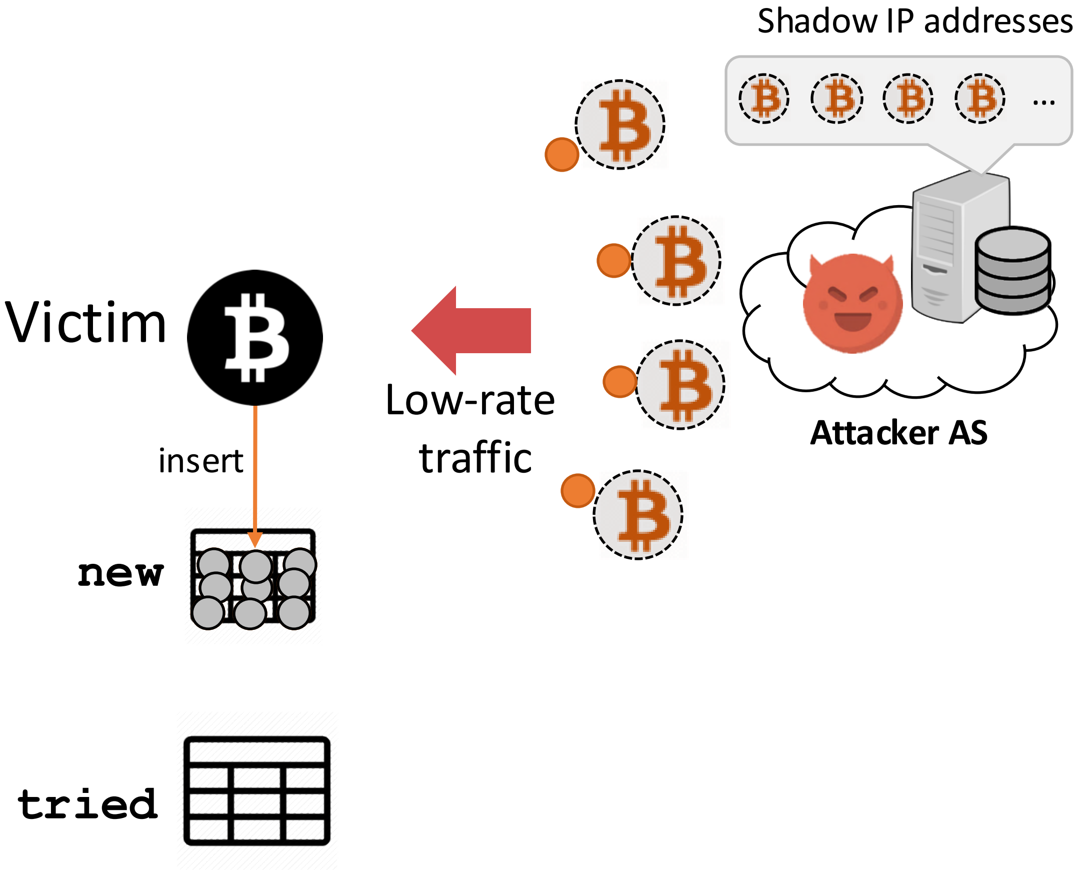
Attack strategy: send ***low-rate*** traffic and ***patiently*** wait



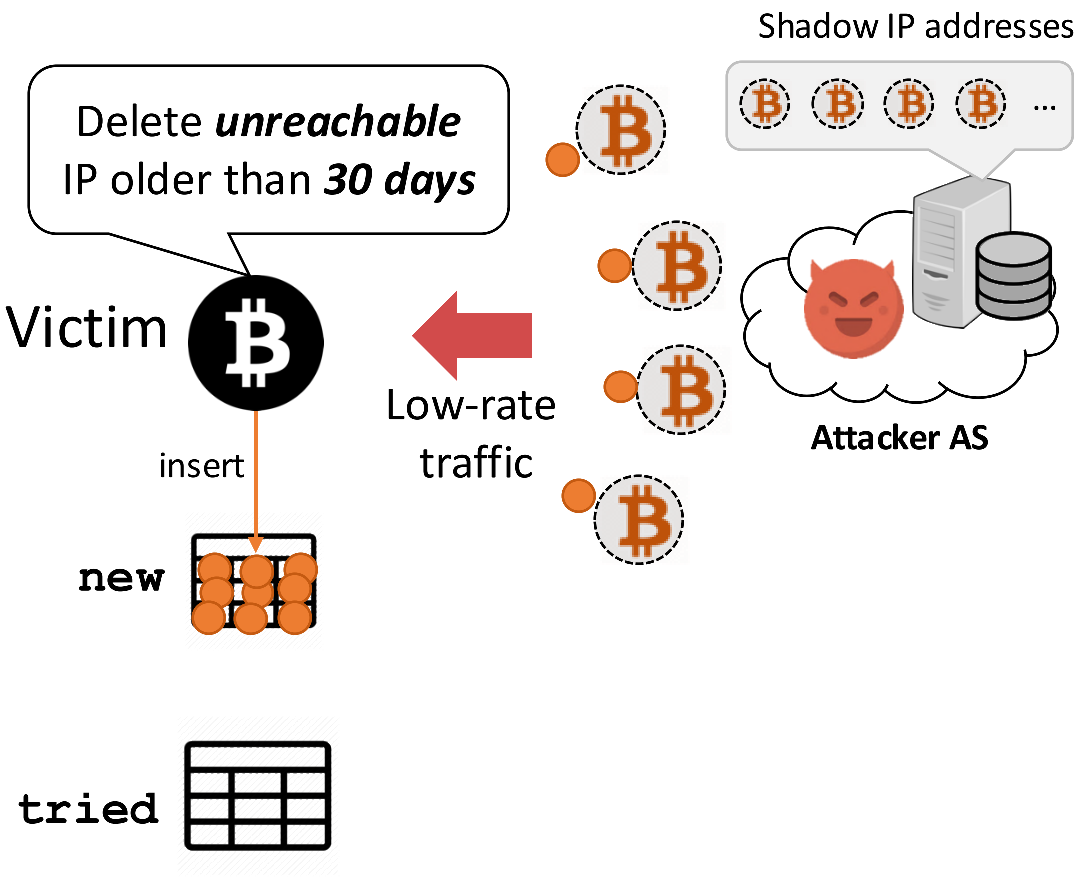
Attack strategy: send ***low-rate*** traffic and ***patiently*** wait



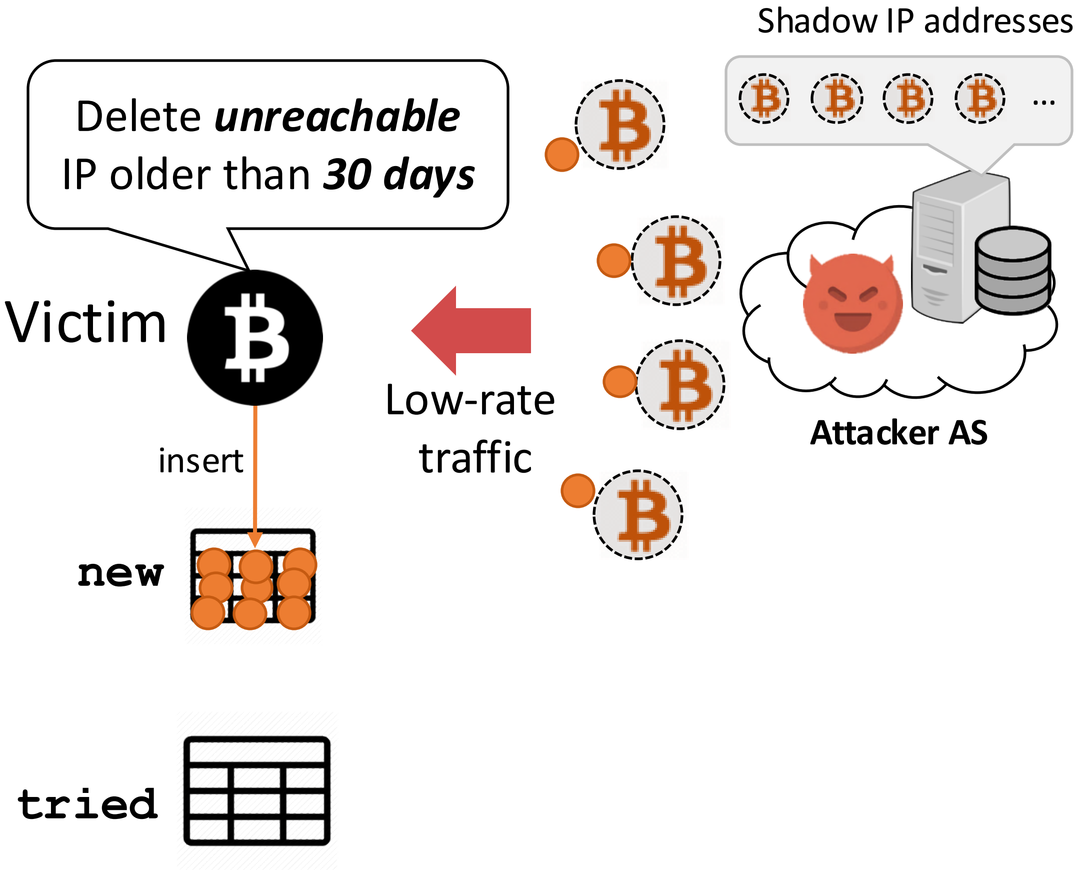
Attack strategy: send *low-rate* traffic and *patiently* wait

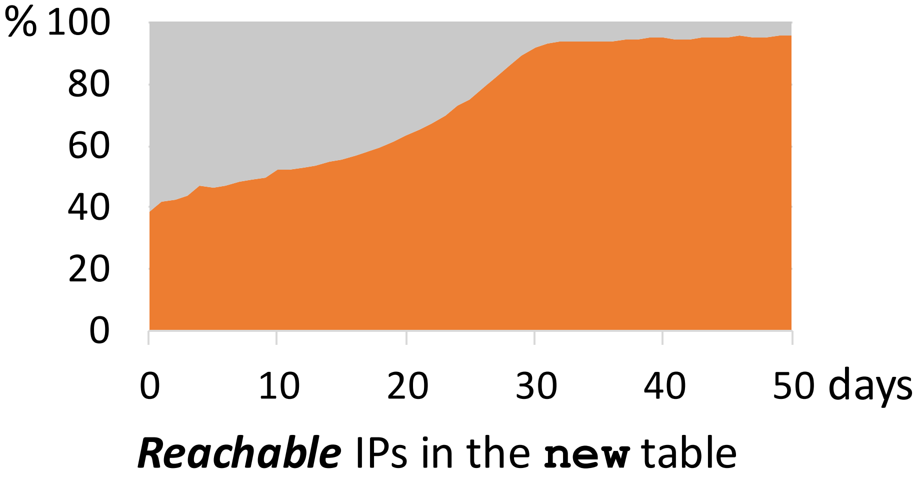


Attack strategy: send ***low-rate*** traffic and ***patiently*** wait

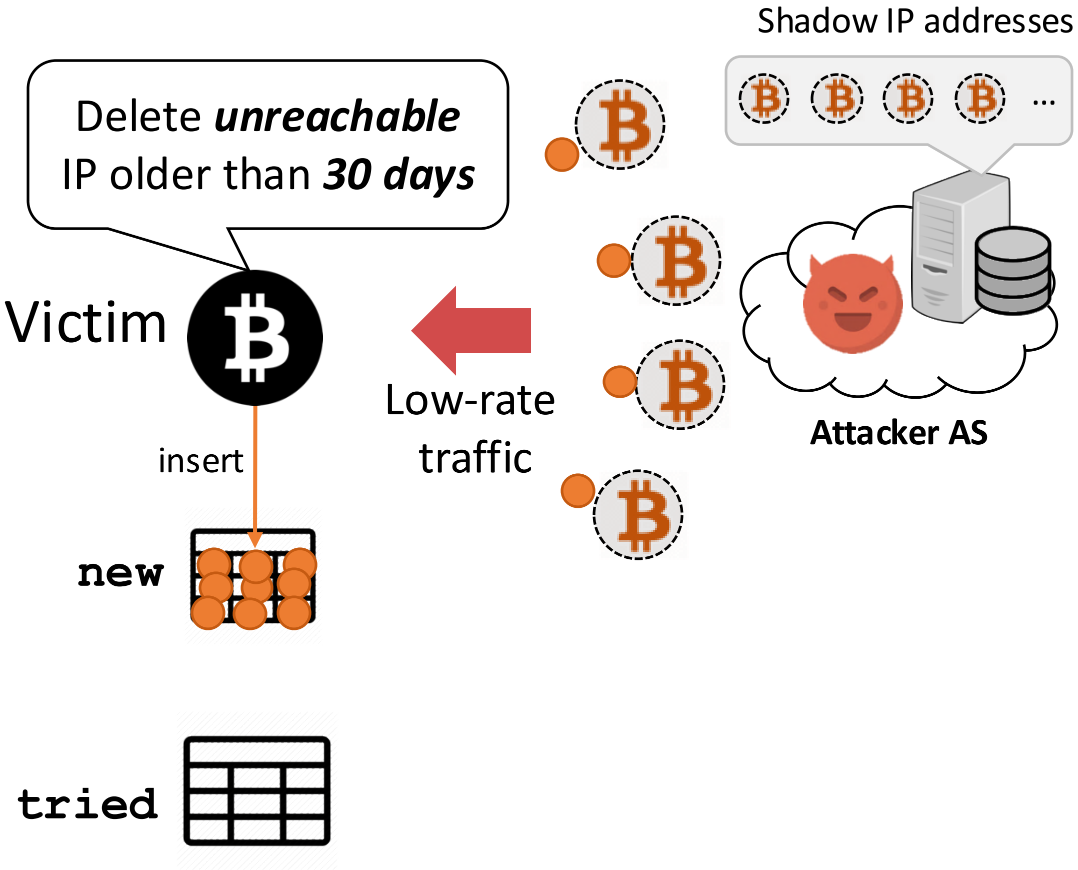


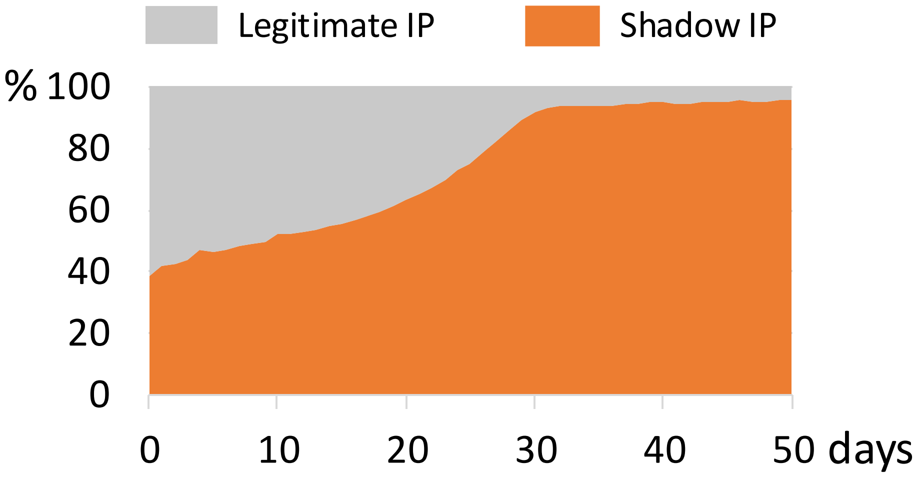
Attack strategy: send ***low-rate*** traffic and ***patiently*** wait





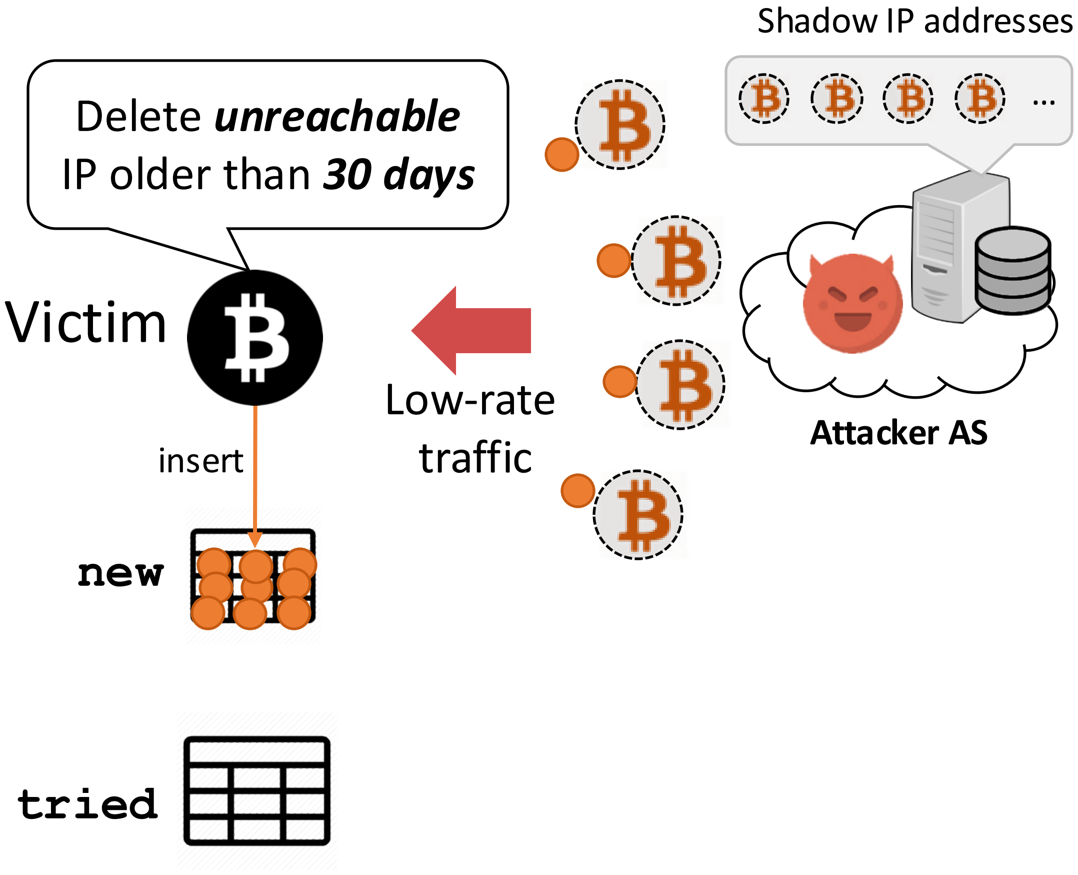
Attack strategy: send ***low-rate*** traffic and ***patiently*** wait

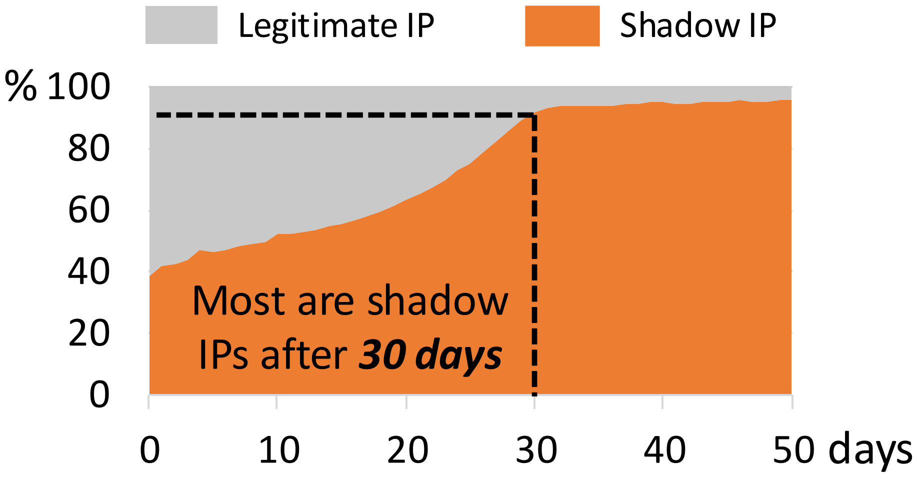




Reachable IPs in the **`new`** table

Attack strategy: send ***low-rate*** traffic and ***patiently*** wait

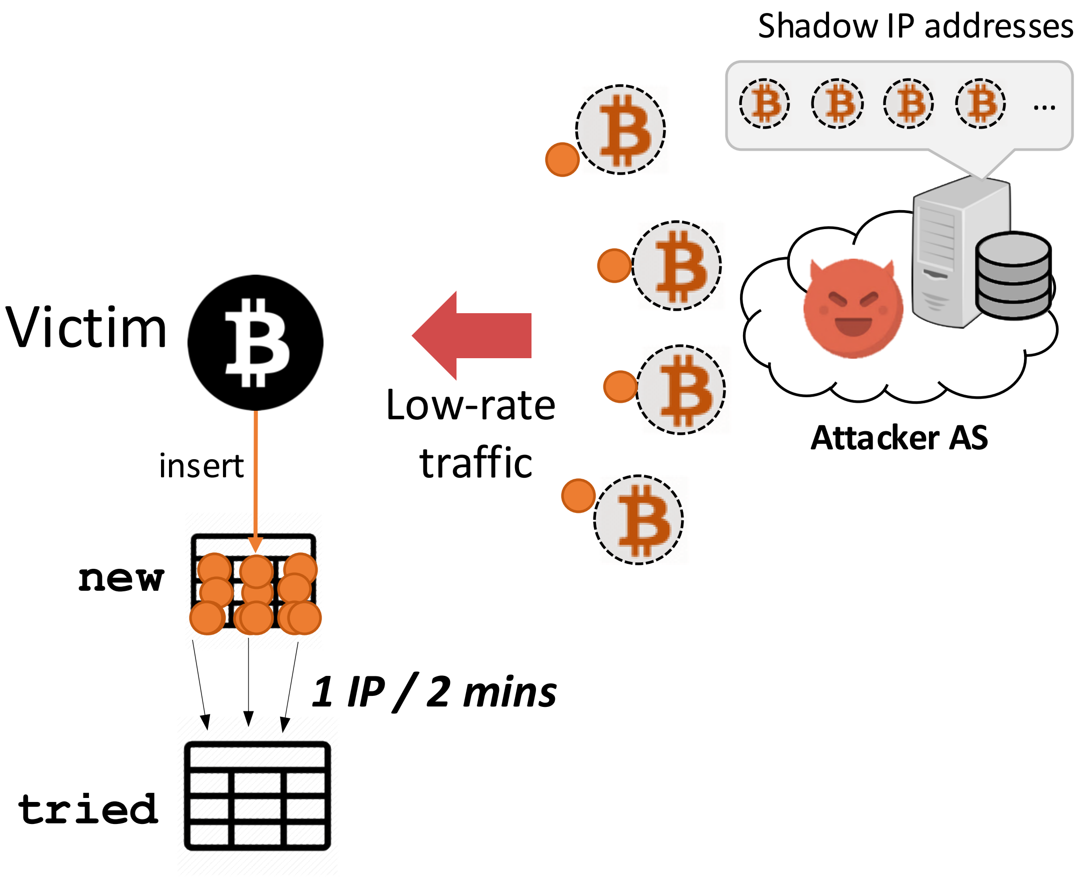

Delete ***unreachable*** IP older than ***30 days***

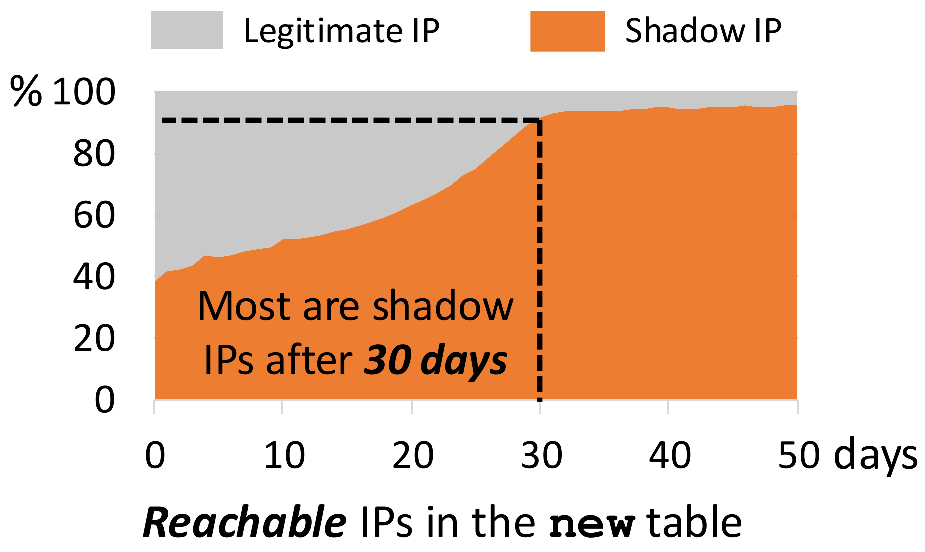


Most are shadow IPs after ***30 days***

Reachable IPs in the **`new`** table

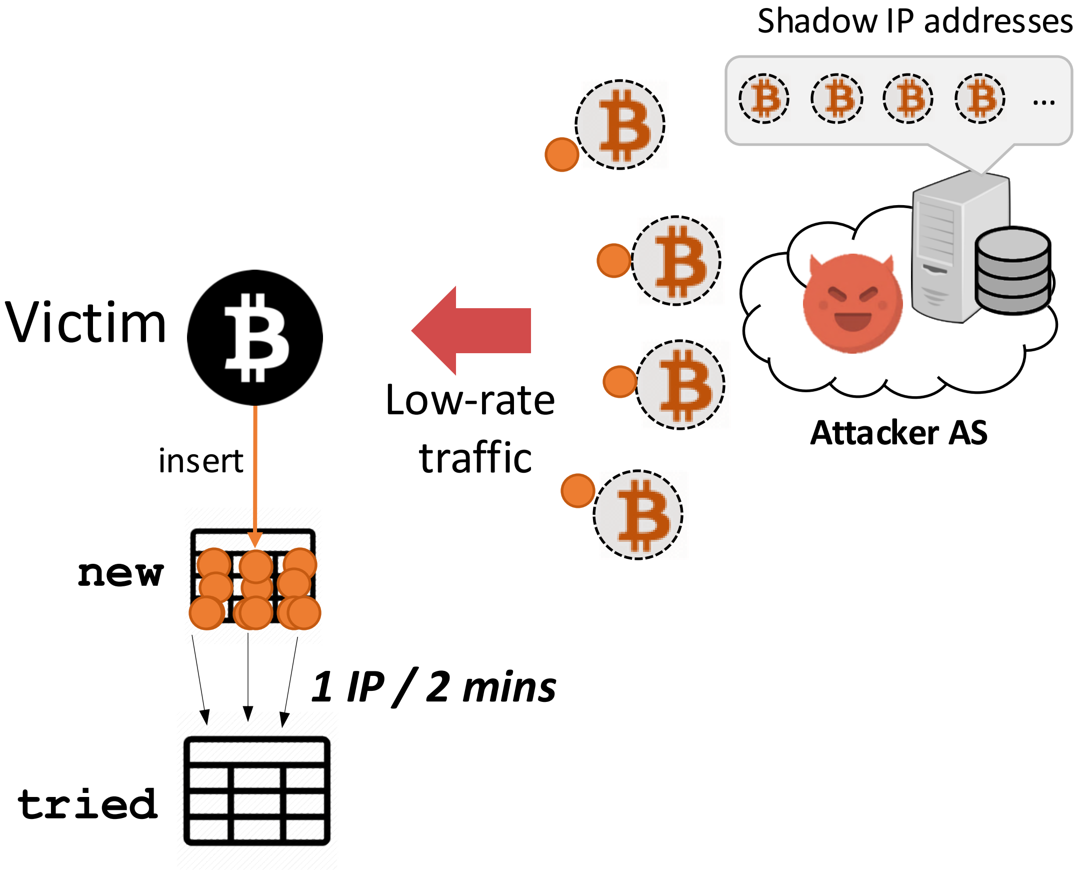
Attack strategy: send ***low-rate*** traffic and ***patiently*** wait

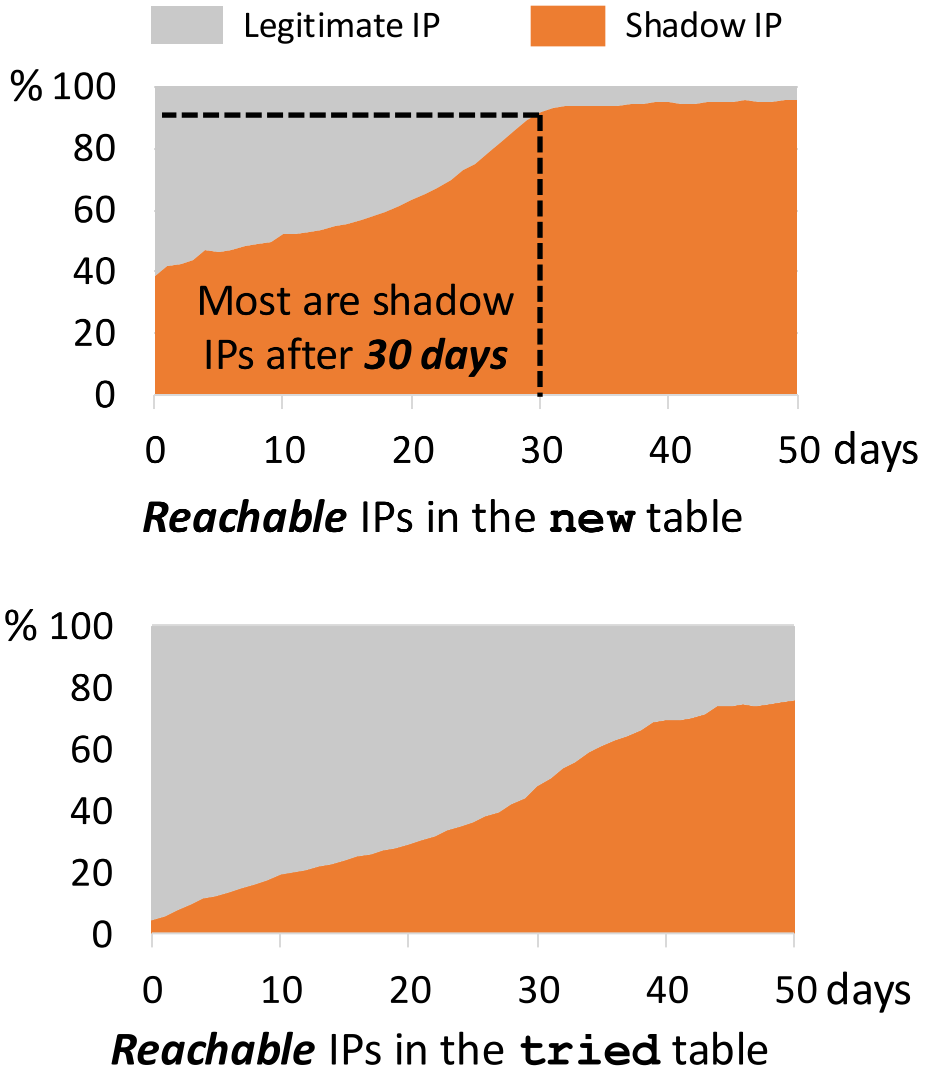




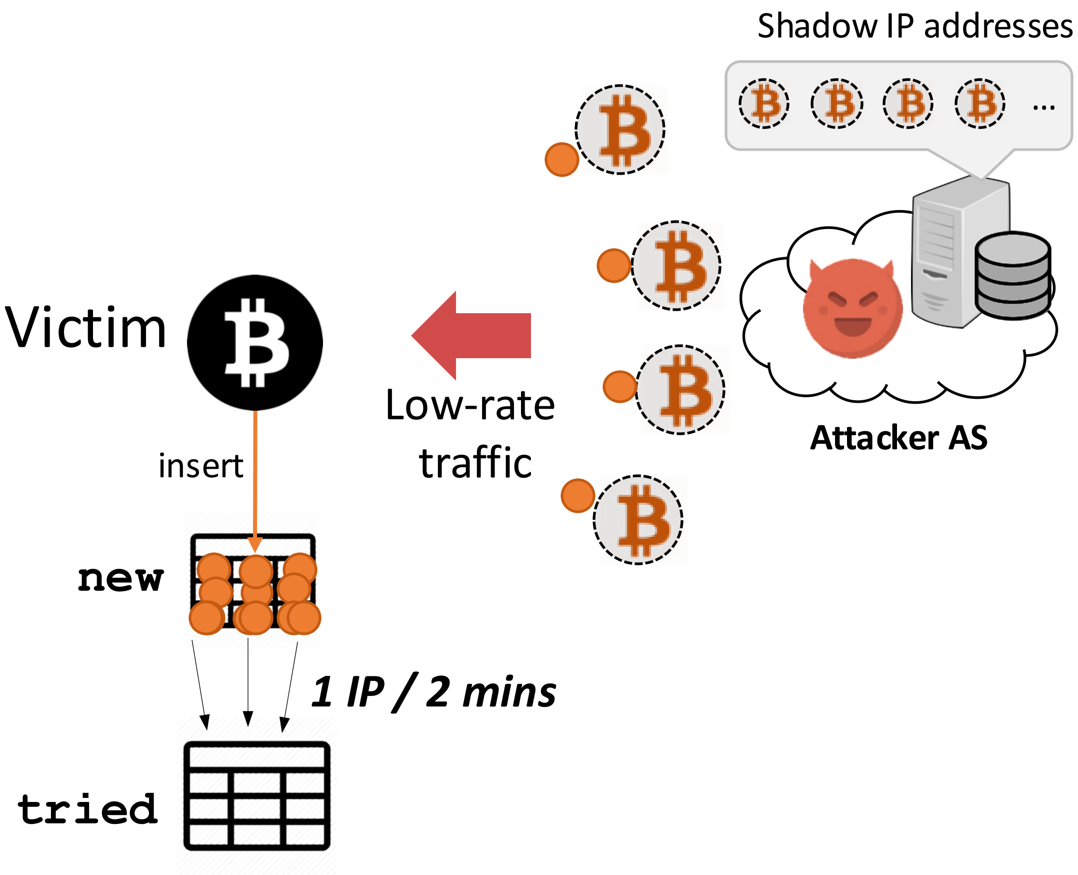
Reachable IPs in the **`new`** table

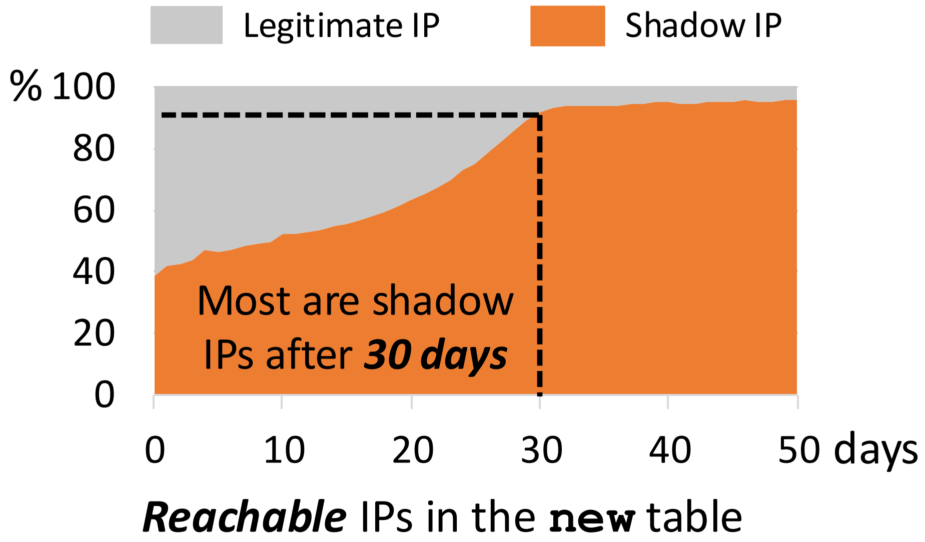
Attack strategy: send ***low-rate*** traffic and ***patiently*** wait



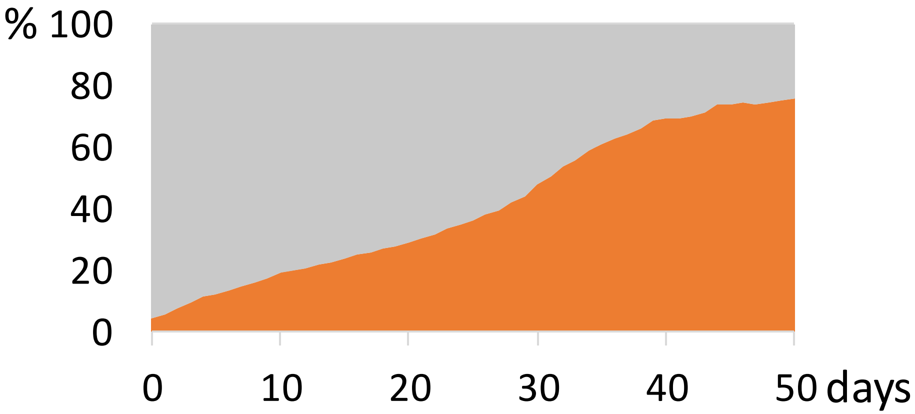


Attack strategy: send *low-rate* traffic and *patiently* wait



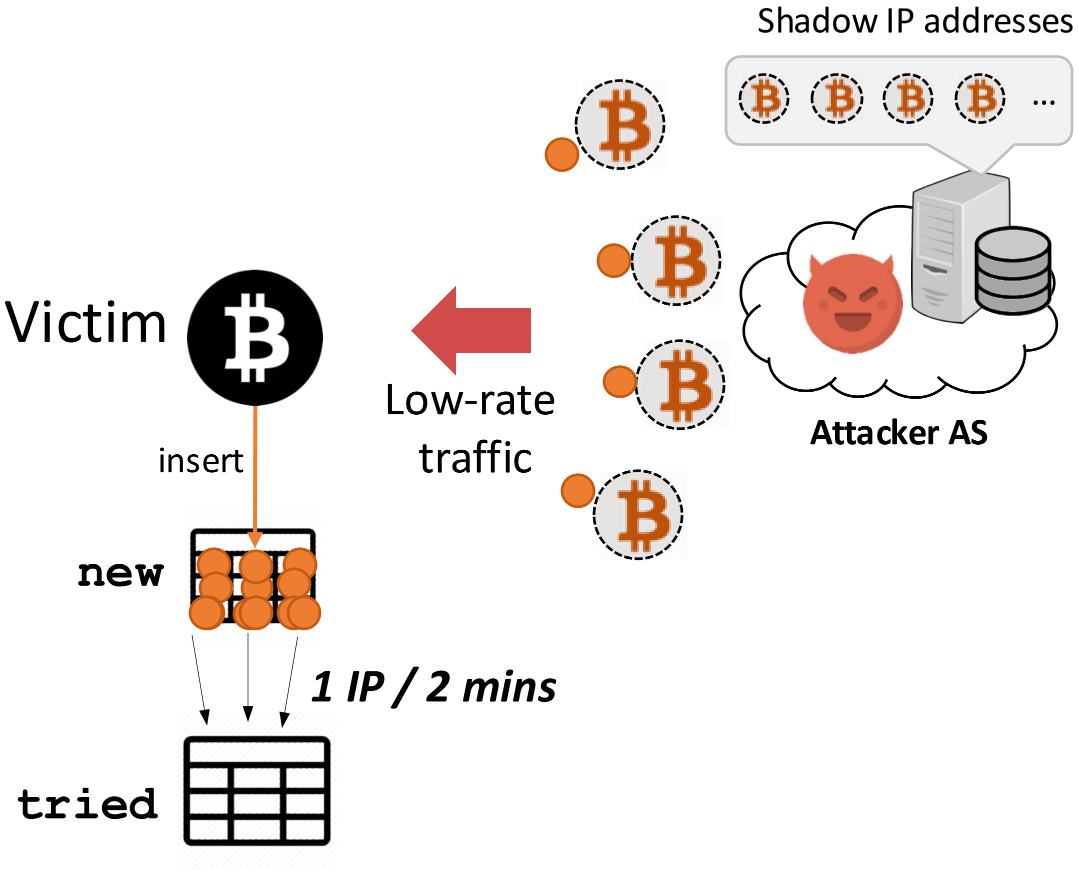


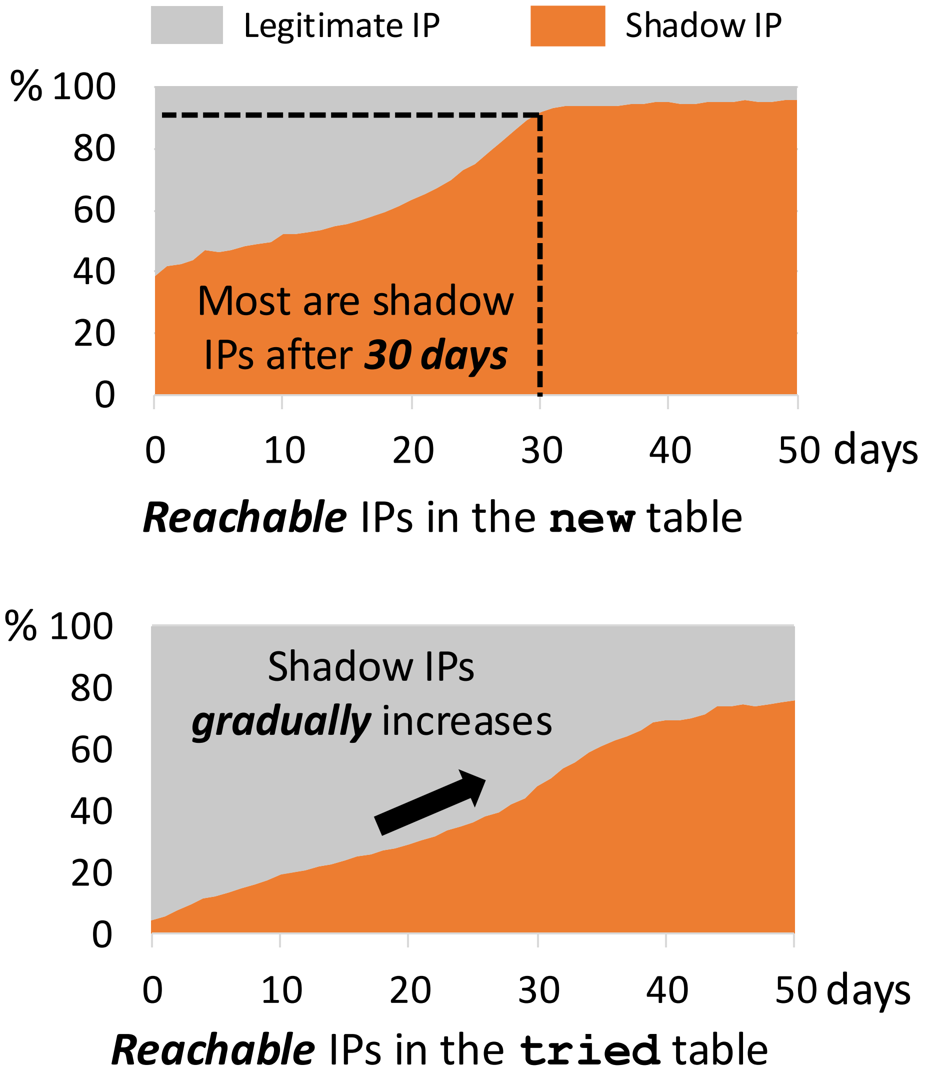
Reachable IPs in the **`new`** table



Reachable IPs in the **`tried`** table

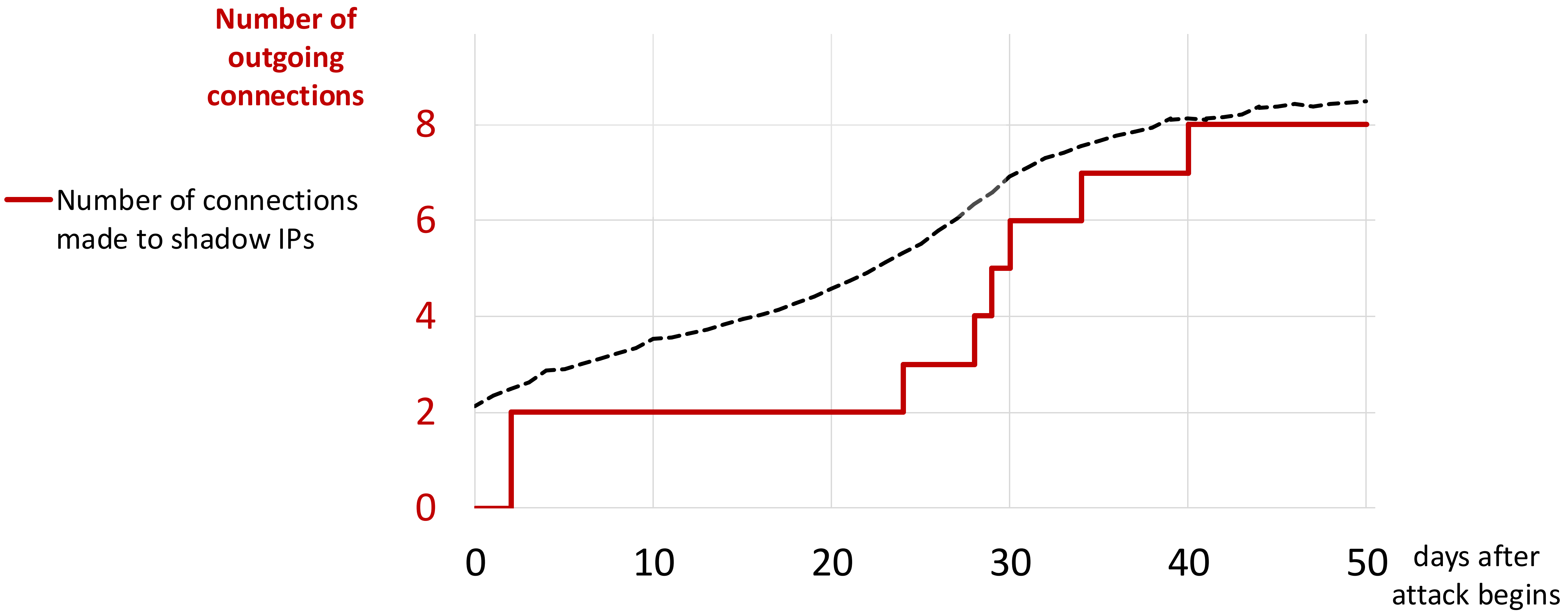
Attack strategy: send ***low-rate*** traffic and ***patiently*** wait



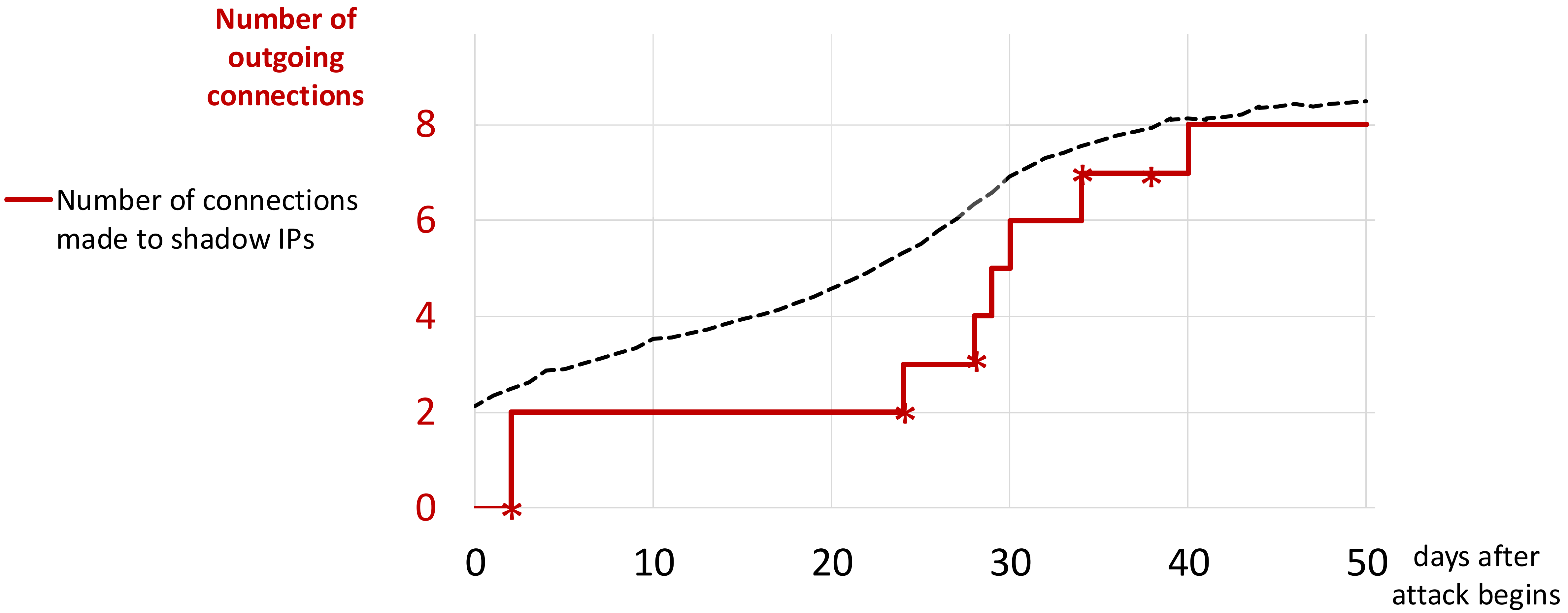


Adversary can occupy ***all*** connections with shadow IPs in ***5 - 6 weeks***

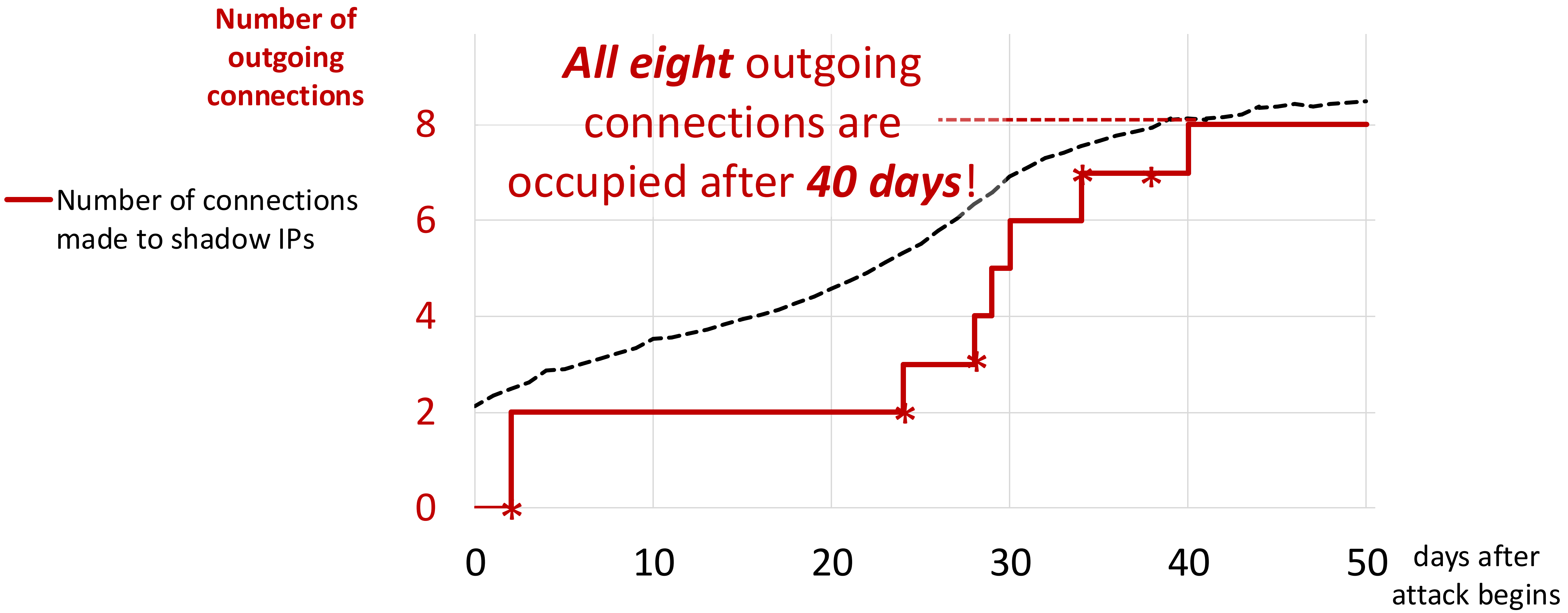
Adversary can occupy ***all*** connections with shadow IPs in ***5 - 6 weeks***



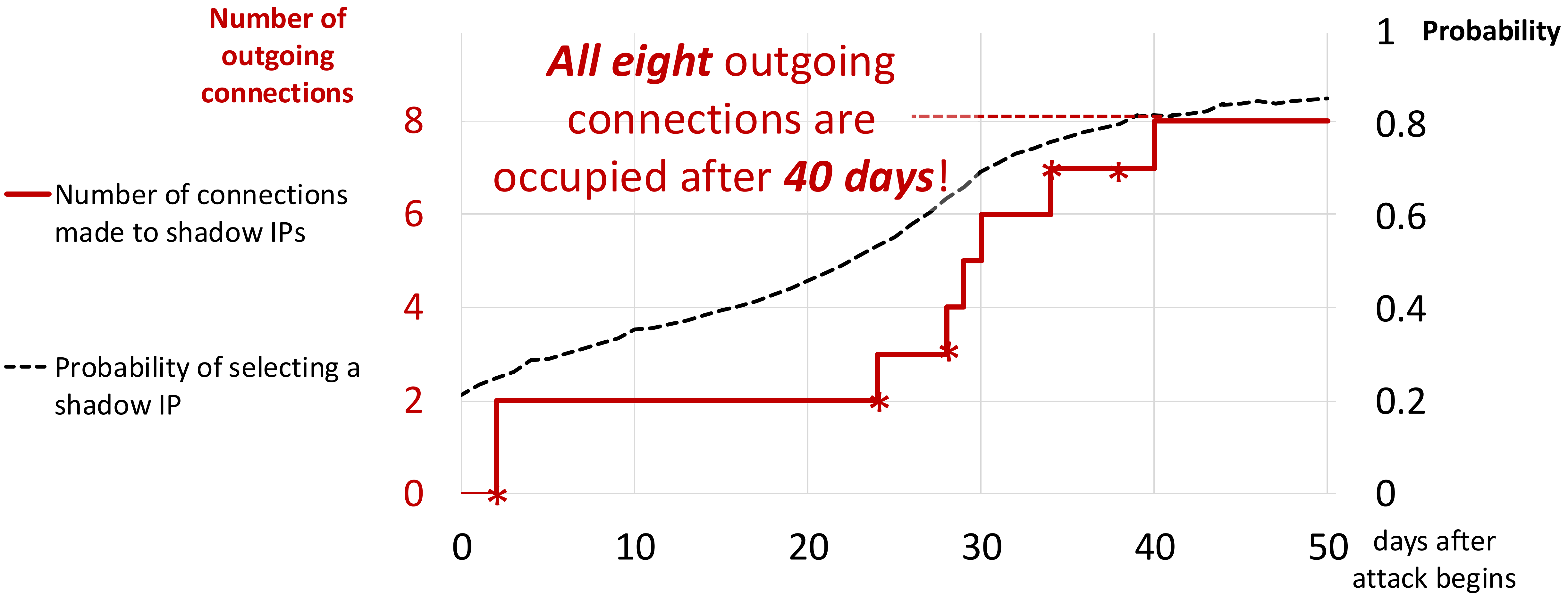
Adversary can occupy ***all*** connections with shadow IPs in ***5 - 6 weeks***



Adversary can occupy ***all*** connections with shadow IPs in ***5 - 6 weeks***



Adversary can occupy ***all*** connections with shadow IPs in ***5 - 6 weeks***



Why is the Erebus attack ***stealthy***?

Why is the Erebus attack ***stealthy***?

- ***No*** route manipulation (e.g., BGP hijacking) needed

Why is the Erebus attack ***stealthy***?

- ***No*** route manipulation (e.g., BGP hijacking) needed

=> ***Invisible*** to control-plane monitors (e.g., BGP collectors)

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

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

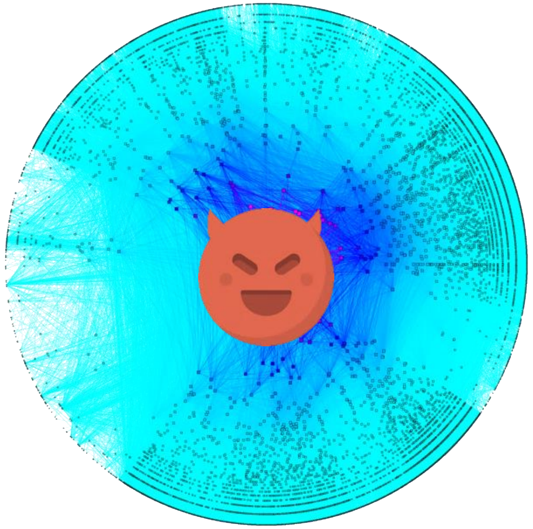
Who can launch the Erebus attack?

Who can launch the Erebus attack?

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

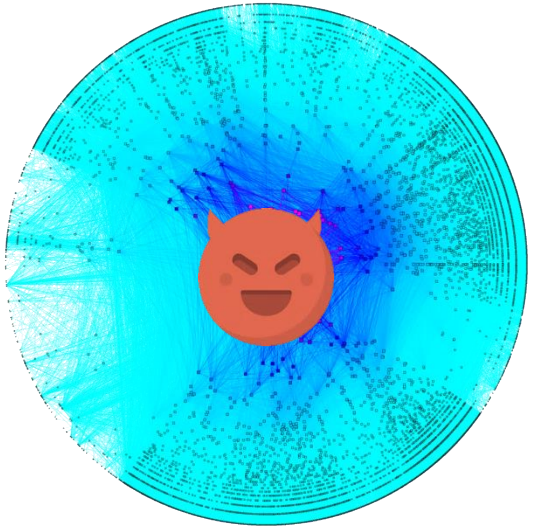
Who can launch the Erebus attack?

- 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!



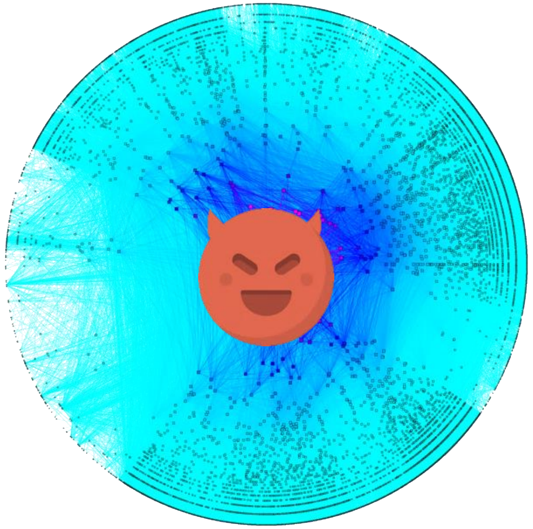
Who can launch the Erebus attack?

- 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!



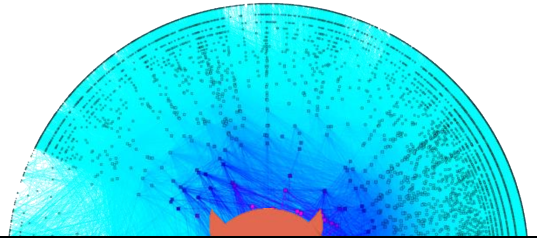
Who can launch the Erebus attack?

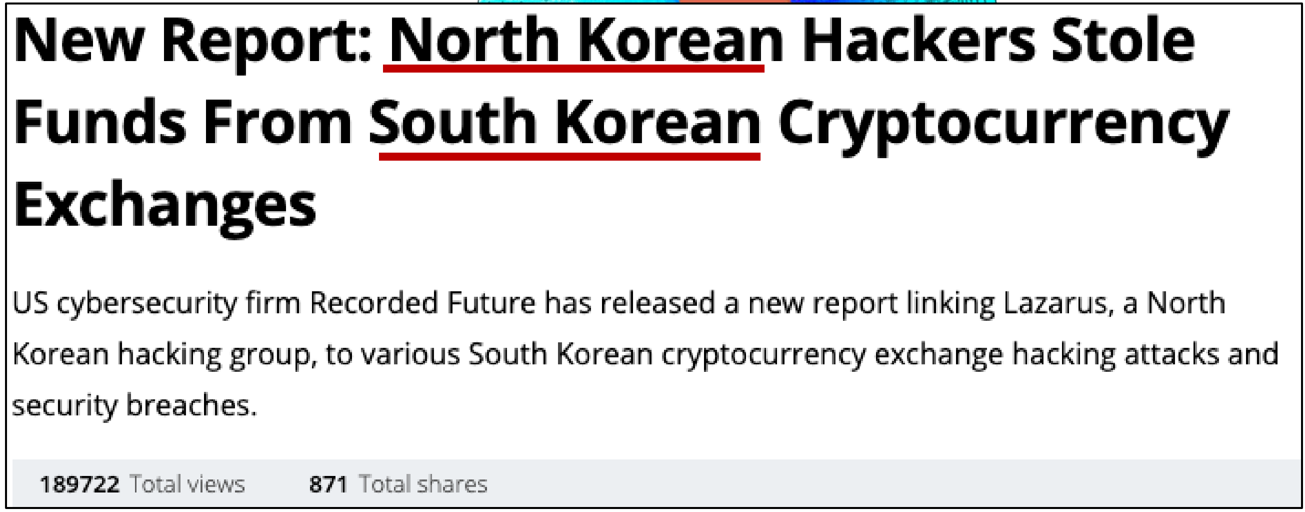
- To attack a targeted node, Erebus attacker needs:
  - ✓***millions*** shadow IP addresses
  - ✓***several weeks*** of attack execution
- ***All Tier-1*** networks
  - ✓AT&T, CenturyLink, NTT, …
  - ✓Can target ***any*** Bitcoin node!
- Many ***large Tier-2*** networks
  - ✓Singtel, China Telecom, …
  - ✓Can target the ***majority*** of nodes!
- ***Nation-state*** adversaries
  - ✓Some countries are believed to have direct control over their ISPs



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.

189722 Total views **871** Total shares

What about other cryptocurrencies?

What about other cryptocurrencies?

bitcoin

- Bitcoin peer-to-peer networking stack is ***widely replicated***

What about other cryptocurrencies?

All vulnerable!

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

Countermeasures against the Erebus attack

Countermeasures against the Erebus attack

- The Erebus attack exploits the ***topological advantage*** of being large ISPs, ***not*** any specific bugs

Countermeasures against the Erebus attack

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

Countermeasures against the Erebus attack

- The Erebus attack exploits the ***topological advantage*** of being large ISPs, ***not*** any specific bugs => ***Hard to counter against!***
- ***Trivial*** (yet ***less practical***) solutions:

Countermeasures against the Erebus attack

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

- ***Trivial*** (yet ***less practical***) solutions:
  - ✓***Trusted*** authority: Whitelist/Blacklist of IPs

Countermeasures against the Erebus attack

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

- ***Trivial*** (yet ***less practical***) solutions:
  - ✓ ***Trusted*** authority: Whitelist/Blacklist of IPs => ***not permissonless***

Countermeasures against the Erebus attack

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

- ***Trivial*** (yet ***less practical***) solutions:
  - ✓***Trusted*** authority: Whitelist/Blacklist of IPs => ***not permissonless***
  - ✓***Third-party*** proxies: VPNs, Tor, relay networks

Countermeasures against the Erebus attack

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

- ***Trivial*** (yet ***less practical***) solutions:
  - ✓***Trusted*** authority: Whitelist/Blacklist of IPs => ***not permissonless***
  - ✓***Third-party*** proxies: VPNs, Tor, relay networks => ***not decentralized***

Countermeasures against the Erebus attack

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

- ***Trivial*** (yet ***less practical***) solutions:
  - ✓***Trusted*** authority: Whitelist/Blacklist of IPs => ***not permissonless***
  - ✓***Third-party*** proxies: VPNs, Tor, relay networks => ***not decentralized***

- ***Partial*** solutions:

Countermeasures against the Erebus attack

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

- ***Trivial*** (yet ***less practical***) solutions:
  - ✓***Trusted*** authority: Whitelist/Blacklist of IPs => ***not permissonless***
  - ✓***Third-party*** proxies: VPNs, Tor, relay networks => ***not decentralized***

- ***Partial*** solutions:
  - ✓Table size ***reduction***

Countermeasures against the Erebus attack

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

- ***Trivial*** (yet ***less practical***) solutions:
  - ✓***Trusted*** authority: Whitelist/Blacklist of IPs => ***not permissonless***
  - ✓***Third-party*** proxies: VPNs, Tor, relay networks => ***not decentralized***

- ***Partial*** solutions:
  - ✓Table size ***reduction***
  - ✓***More*** outgoing connections

Countermeasures against the Erebus attack

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

- ***Trivial*** (yet ***less practical***) solutions:
  - ✓***Trusted*** authority: Whitelist/Blacklist of IPs => ***not permissonless***
  - ✓***Third-party*** proxies: VPNs, Tor, relay networks => ***not decentralized***

- ***Partial*** solutions:
  - ✓Table size ***reduction***
  - ✓***More*** outgoing connections

Deployed in the latest version

Countermeasures against the Erebus attack

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

- ***Trivial*** (yet ***less practical***) solutions:
  - ✓***Trusted*** authority: Whitelist/Blacklist of IPs => ***not permissonless***
  - ✓***Third-party*** proxies: VPNs, Tor, relay networks => ***not decentralized***

- ***Partial*** solutions:
  - ✓Table size ***reduction***
  - ✓***More*** outgoing connections
  - ✓Incorporating ***AS topology*** in the peer selection

Deployed in the latest version

Countermeasures against the Erebus attack

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

- ***Trivial*** (yet ***less practical***) solutions:
  - ✓***Trusted*** authority: Whitelist/Blacklist of IPs => ***not permissonless***
  - ✓***Third-party*** proxies: VPNs, Tor, relay networks => ***not decentralized***

- ***Partial*** solutions:
  - ✓Table size ***reduction***
  - ✓***More*** outgoing connections *Deployed in the latest version*
  - ✓Incorporating ***AS topology*** in the peer selection *Being tested*

Countermeasures against the Erebus attack

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

- ***Trivial*** (yet ***less practical***) solutions:
  - ✓***Trusted*** authority: Whitelist/Blacklist of IPs => ***not permissonless***
  - ✓***Third-party*** proxies: VPNs, Tor, relay networks => ***not decentralized***

- ***Partial*** solutions:
  - ✓Table size ***reduction***
  - ✓***More*** outgoing connections *Deployed in the latest version*
  - ✓Incorporating ***AS topology*** in the peer selection *Being tested*
  - ✓Protecting peers providing ***fresher*** block data *Being tested*

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.**

- ***Partial*** solutions:
  - ✓Table size ***reduction***
  - ✓***More*** outgoing connections — *Deployed in the latest version*
  - ✓Incorporating ***AS topology*** in the peer selection — *Being tested*
  - ✓Protecting peers providing ***fresher*** block data — *Being tested*

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 — *Deployed in the latest version*
  - ✓Incorporating ***AS topology*** in the peer selection — *Being tested*
  - ✓Protecting peers providing ***fresher*** block data — *Being tested*

Conclusions

EREBUS

Conclusions

- Erebus attack can isolate Bitcoin nodes in a ***stealthy*** manner

Conclusions

EREBUS

- 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

Conclusions

EREBUS

- 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***

Conclusions

EREBUS

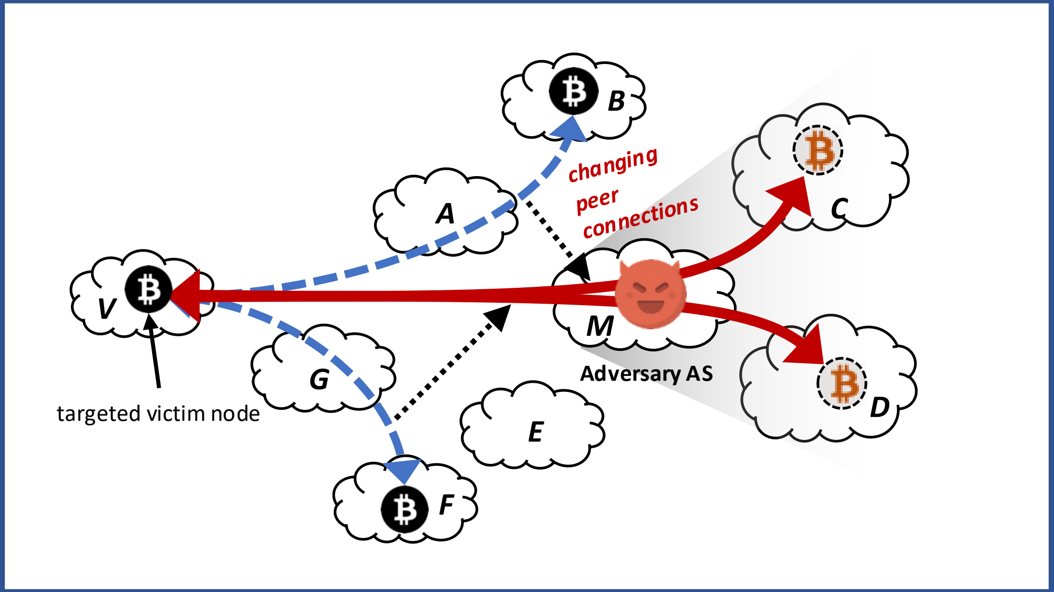
- Erebus attack can isolate Bitcoin nodes in a ***stealthy*** manner
  - ✓***Low rate*** attack traffic (520 bit/s per node)
  - ✓Patiently waiting for ***a few weeks***
  - ✓Large ISPs can launch this attack against latest Bitcoin Core
- Mitigating the Erebus attack is ***hard***
  - ✓***No*** software bugs was exploited
  - ✓Attackers only exploit the ***topological advantages*** of being ISPs

Conclusions

EREBUS

- 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

NUS National University of Singapore

EREBUS