Investigando as Implicações de Segurança da Engenharia de Tráfego e Conectividade no Roteamento da Internet

Renan Barreto
renan.barreto@furg.br

Orientador: Pedro Marcos
Coorientador: Leandro Bertholdo

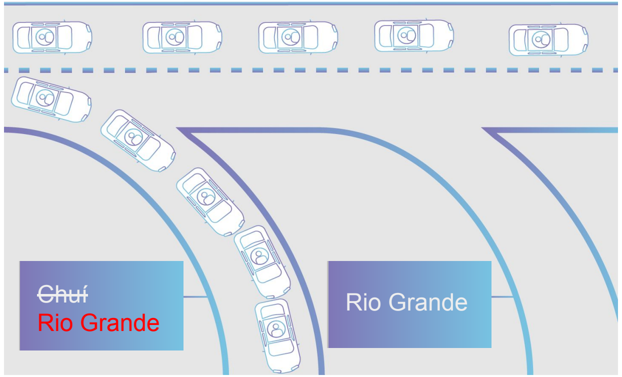
FURG
UNIVERSIDADE FEDERAL
DO RIO GRANDE

Dezembro de 2025

C3
centro de
ciências
computacionais

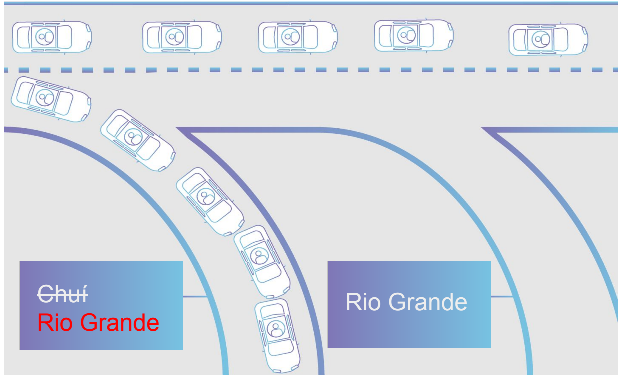
Eventos de Sequestro de Prefixo afetam a Internet

Eventos de Sequestro de Prefixo afetam a Internet

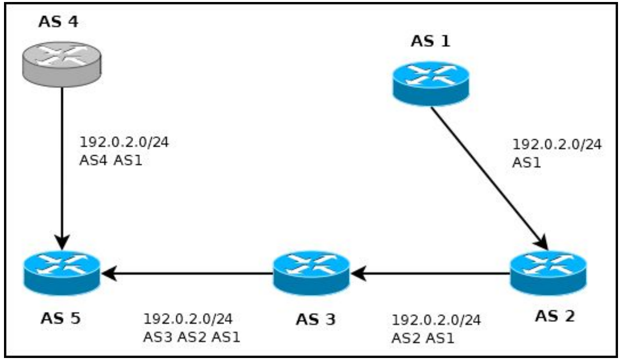


Ocorrem quando um AS anuncia um Prefixo que ele não é dono

Eventos de Sequestro de Prefixo afetam a Internet

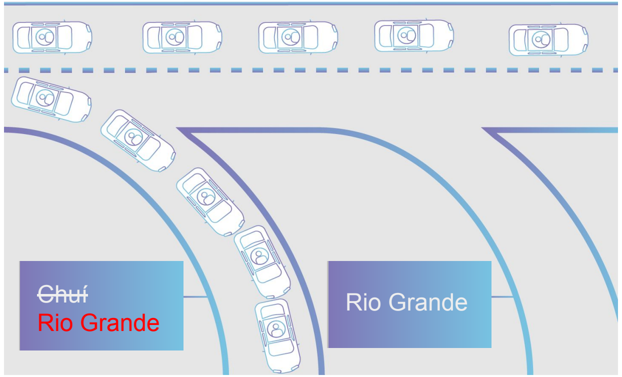


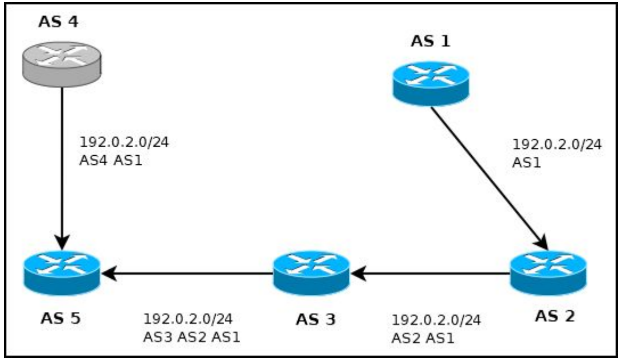
Ocorrem quando um AS anuncia um Prefixo que ele não é dono



Quando um AS anuncia um caminho para outro AS, o qual ele não possui

Eventos de Sequestro de Prefixo afetam a Internet



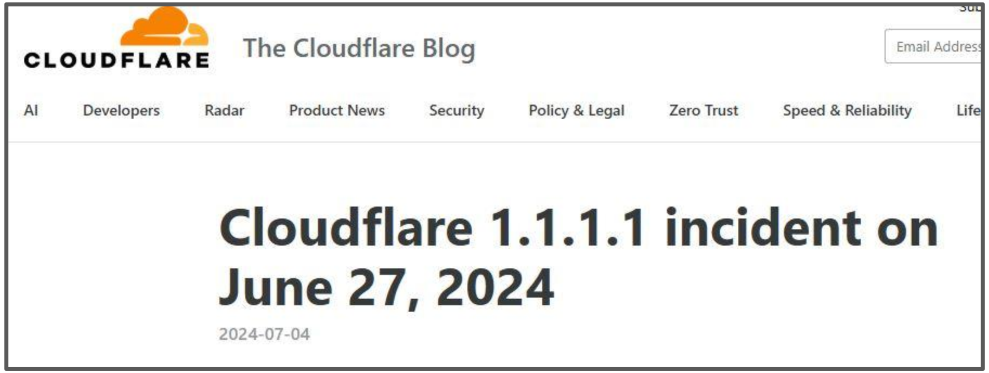


Ocorrem quando um AS anuncia um Prefixo que ele não é dono

Quando um AS anuncia um caminho para outro AS, o qual ele não possui

ASes maliciosos podem atrasar, descartar ou interceptar informações

Eventos de Sequestro de Prefixo afetam a Internet

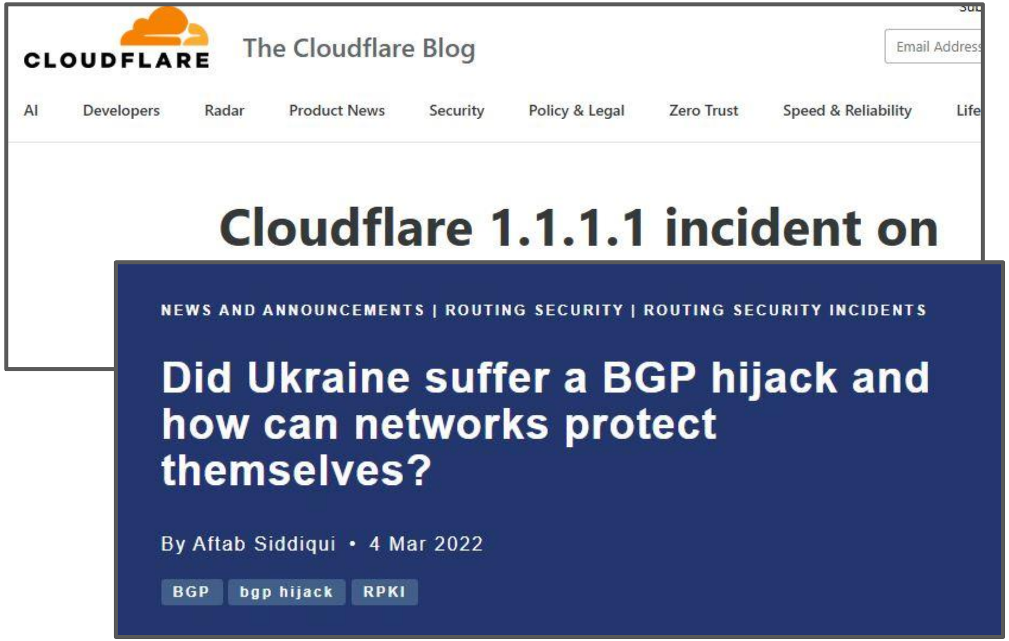


Cloudflare 1.1.1.1 incident on June 27, 2024

2024-07-04

ASes maliciosos podem atrasar, descartar ou interceptar informações

Eventos de Sequestro de Prefixo afetam a Internet



Cloudflare 1.1.1.1 incident on

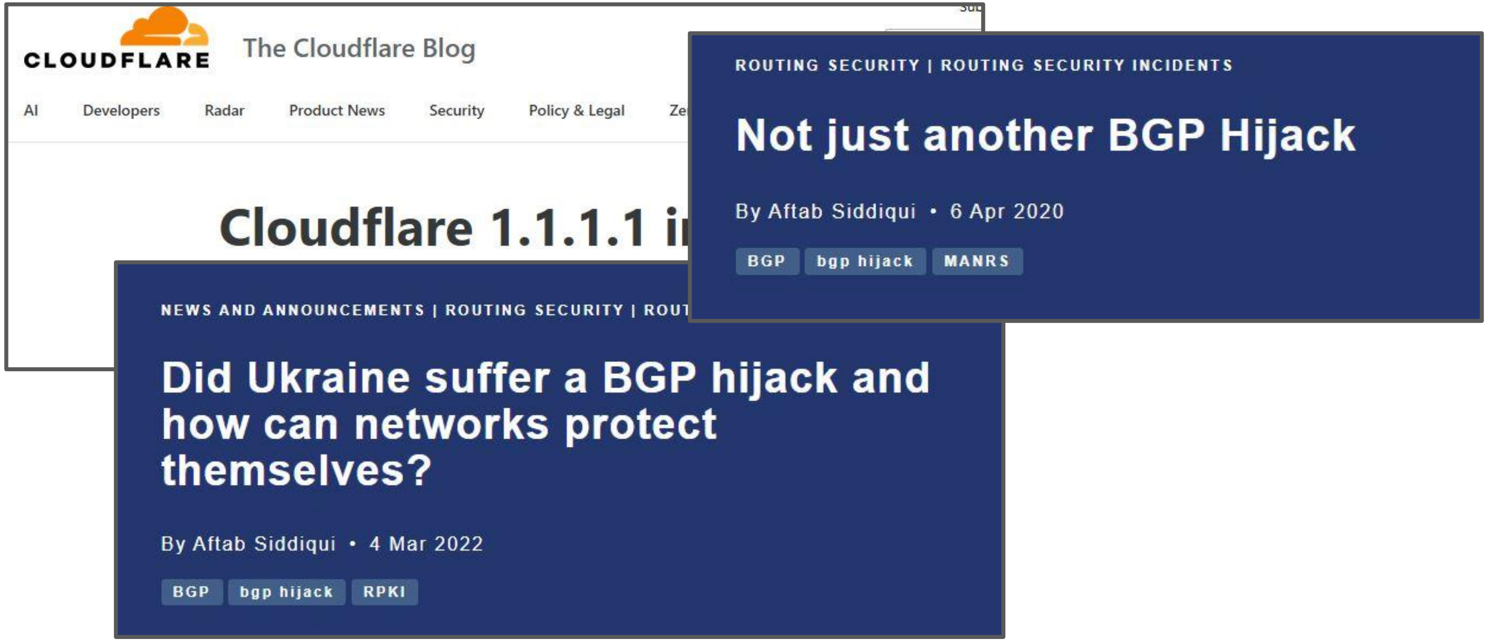
NEWS AND ANNOUNCEMENTS | ROUTING SECURITY | ROUTING SECURITY INCIDENTS

Did Ukraine suffer a BGP hijack and how can networks protect themselves?

By Aftab Siddiqui • 4 Mar 2022

ASes maliciosos podem atrasar, descartar ou interceptar informações

Eventos de Sequestro de Prefixo afetam a Internet



CLOUDFLARE The Cloudflare Blog

AI Developers Radar Product News Security Policy & Legal Ze

Cloudflare 1.1.1.1 i

ROUTING SECURITY | ROUTING SECURITY INCIDENTS

Not just another BGP Hijack

By Aftab Siddiqui • 6 Apr 2020

BGP bgp hijack MANRS

NEWS AND ANNOUNCEMENTS | ROUTING SECURITY | ROUT

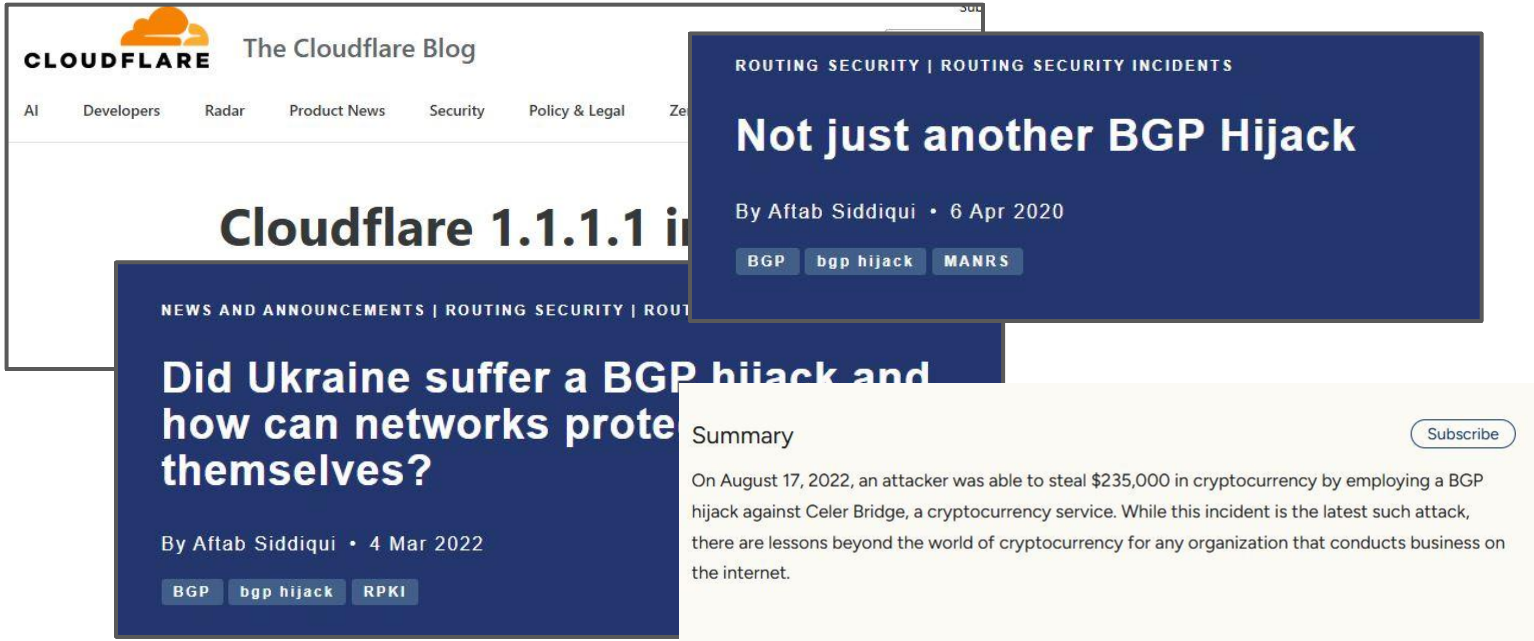
Did Ukraine suffer a BGP hijack and how can networks protect themselves?

By Aftab Siddiqui • 4 Mar 2022

BGP bgp hijack RPKI

ASes maliciosos podem atrasar, descartar ou interceptar informações

Eventos de Sequestro de Prefixo afetam a Internet



Cloudflare 1.1.1.1 i

ROUTING SECURITY | ROUTING SECURITY INCIDENTS

Not just another BGP Hijack

By Aftab Siddiqui • 6 Apr 2020

NEWS AND ANNOUNCEMENTS | ROUTING SECURITY | ROUT

Did Ukraine suffer a BGP hijack and how can networks prote themselves?

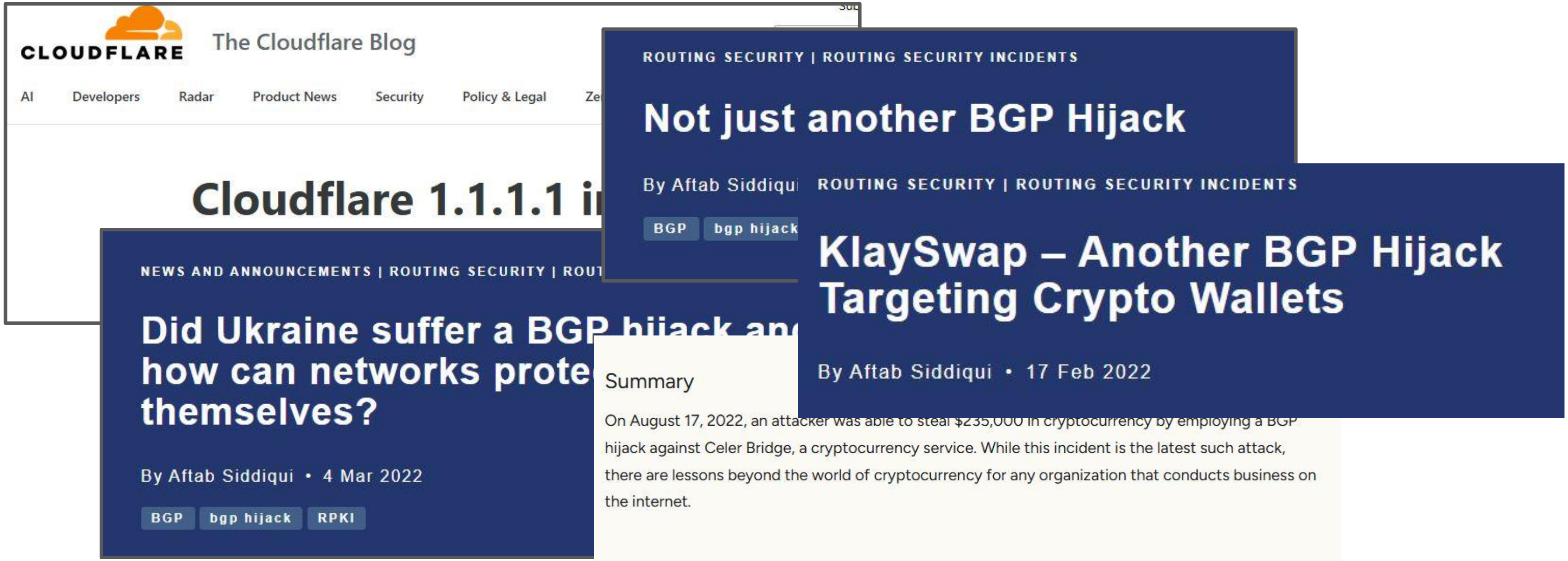
By Aftab Siddiqui • 4 Mar 2022

Summary

On August 17, 2022, an attacker was able to steal $235,000 in cryptocurrency by employing a BGP hijack against Celer Bridge, a cryptocurrency service. While this incident is the latest such attack, there are lessons beyond the world of cryptocurrency for any organization that conducts business on the internet.

ASes maliciosos podem atrasar, descartar ou interceptar informações

Eventos de Sequestro de Prefixo afetam a Internet



CLOUDFLARE The Cloudflare Blog

AI Developers Radar Product News Security Policy & Legal Ze

Cloudflare 1.1.1.1 i

ROUTING SECURITY | ROUTING SECURITY INCIDENTS

Not just another BGP Hijack

By Aftab Siddiqui

BGP bgp hijack

NEWS AND ANNOUNCEMENTS | ROUTING SECURITY | ROUT

Did Ukraine suffer a BGP hijack an how can networks prote themselves?

By Aftab Siddiqui • 4 Mar 2022

BGP bgp hijack RPKI

ROUTING SECURITY | ROUTING SECURITY INCIDENTS

KlaySwap – Another BGP Hijack Targeting Crypto Wallets

By Aftab Siddiqui • 17 Feb 2022

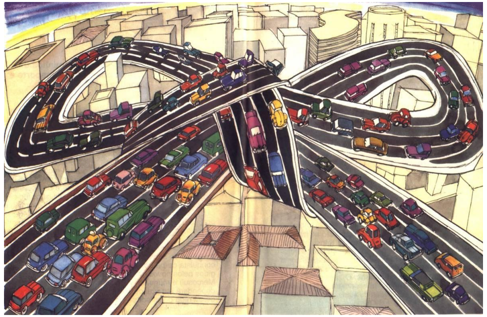
Summary

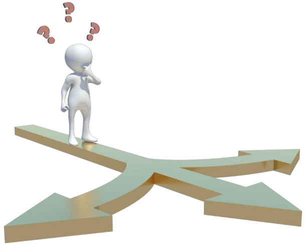
On August 17, 2022, an attacker was able to steal $235,000 in cryptocurrency by employing a BGP hijack against Celer Bridge, a cryptocurrency service. While this incident is the latest such attack, there are lessons beyond the world of cryptocurrency for any organization that conducts business on the internet.

ASes maliciosos podem atrasar, descartar ou interceptar informações

A Otimização da troca de tráfego entre ASes é uma necessidade

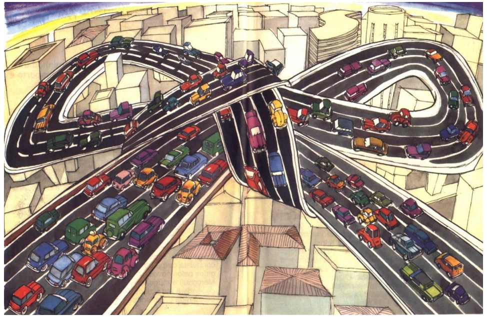
A Otimização da troca de tráfego entre ASes é uma necessidade

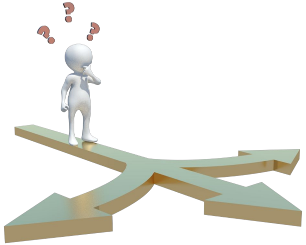




Cada vez mais tráfego, rotas e ASes

A Otimização da troca de tráfego entre ASes é uma necessidade





Cada vez mais tráfego, rotas e ASes

Engenharia de Tráfego busca solucionar o problema da otimização

Tráfego de entrada

- Influenciar

Tráfego de entrada

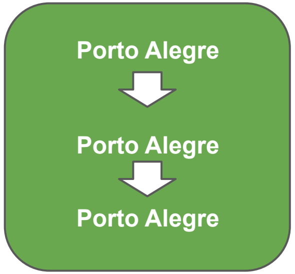
- Influenciar
- Técnicas de Engenharia de Tráfego

Tráfego de entrada

- Influenciar
- Técnicas de Engenharia de Tráfego
- Iremos focar no Tráfego de Entrada

Tráfego de entrada

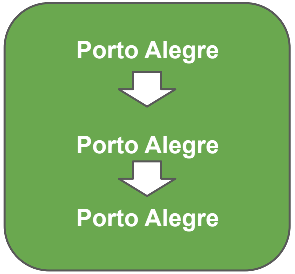
- Influenciar
- Técnicas de Engenharia de Tráfego
- Iremos focar no Tráfego de Entrada



Prepend…

Tráfego de entrada

- Influenciar
- Técnicas de Engenharia de Tráfego
- Iremos focar no Tráfego de Entrada



Porto Alegre

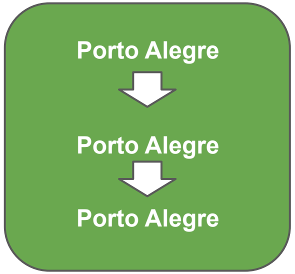
Porto Alegre

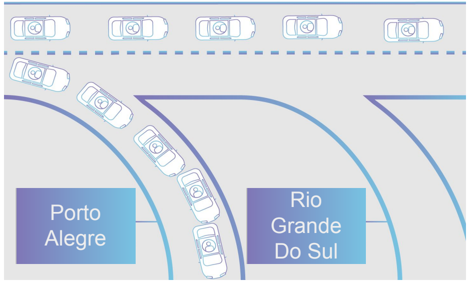
Porto Alegre

Prepend, Anúncios Seletivos …

Tráfego de entrada

- Influenciar
- Técnicas de Engenharia de Tráfego
- Iremos focar no Tráfego de Entrada

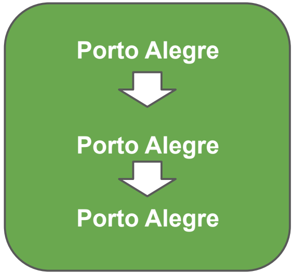




Prepend, Anúncios Seletivos, Anúncios Específicos,…

Tráfego de entrada

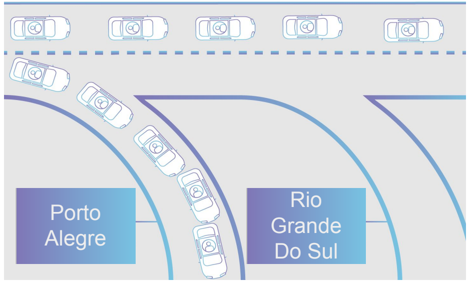
- Influenciar
- Técnicas de Engenharia de Tráfego
- Iremos focar no Tráfego de Entrada

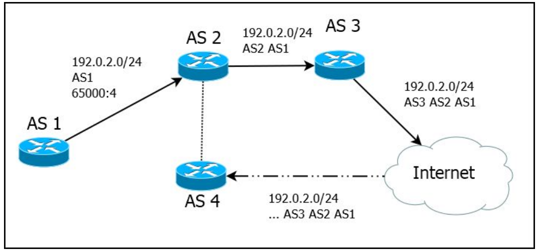


Porto Alegre

Porto Alegre

Porto Alegre





Prepend, Anúncios Seletivos, Anúncios Específicos, Comunidades BGP ...

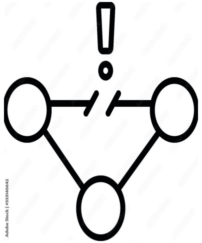
Entre os problemas das Técnicas de Engenharia de Tráfego estão

Entre os problemas das Técnicas de Engenharia de Tráfego estão

Desagregação
Leva ao Aumento
das RIBs

Entre os problemas das Técnicas de Engenharia de Tráfego estão

Desagregação
Leva ao Aumento
das RIBs



Anúncio Seletivo
pode Diminuir
Resiliência

Entre os problemas das Técnicas de Engenharia de Tráfego estão

Desagregação Leva ao Aumento das RIBs

Anúncio Seletivo pode Diminuir Resiliência

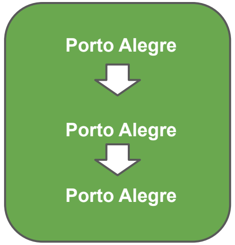
Comunidades BGP Não Possuem Padronização

Entre os problemas das Técnicas de Engenharia de Tráfego estão

Desagregação Leva ao Aumento das RIBs

Anúncio Seletivo pode Diminuir Resiliência

Comunidades BGP Não Possuem Padronização



Porto Alegre

Porto Alegre

Porto Alegre

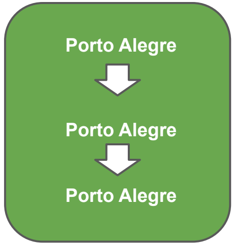
Prepend pode aumentar riscos de segurança

Entre os problemas das Técnicas de Engenharia de Tráfego estão

Desagregação Leva ao Aumento das RIBs

Anúncio Seletivo pode Diminuir Resiliência

Comunidades BGP Não Possuem Padronização



Prepend pode aumentar riscos de segurança

Outro problema é a suscetibilidade a Eventos de Sequestro de Prefixo

Nosso Objetivo

Nosso objetivo é compreender o impacto das Técnicas de Engenharia de Tráfego na Segurança do Roteamento da Internet com as seguintes questões de pesquisa:

Nosso objetivo é compreender o impacto das Técnicas de Engenharia de Tráfego na Segurança do Roteamento da Internet com as seguintes questões de pesquisa:

RQ1:Como diferentes técnicas aumentam a afetam o impacto de um sequestro?

Nosso objetivo é compreender o impacto das Técnicas de Engenharia de Tráfego na Segurança do Roteamento da Internet com as seguintes questões de pesquisa:

RQ1:Como diferentes técnicas aumentam a afetam o impacto de um sequestro?

RQ2-3:Quais características da vítima influenciam o resultado do sequestro? e do atacante?

Nosso objetivo é compreender o impacto das Técnicas de Engenharia de Tráfego na Segurança do Roteamento da Internet com as seguintes questões de pesquisa:

RQ1:Como diferentes técnicas aumentam a afetam o impacto de um sequestro?

RQ2-3:Quais características da vítima influenciam o resultado do sequestro? e do atacante?

RQ4:O que leva um AS a aceitar o anúncio de um sequestro?

Nosso objetivo é compreender o impacto das Técnicas de Engenharia de Tráfego na Segurança do Roteamento da Internet com as seguintes questões de pesquisa:

RQ1:Como diferentes técnicas aumentam a afetam o impacto de um sequestro?

RQ2-3:Quais características da vítima influenciam o resultado do sequestro? e do atacante?

RQ4:O que leva um AS a aceitar o anúncio de um sequestro?

RQ5:Qual o estado atual de uso de ITE e o possível impacto na segurança?

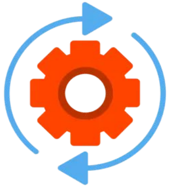
Para atingir este objetivo precisamos:

Para atingir este objetivo precisamos:

Verificar Trabalhos Anteriores

Para atingir este objetivo precisamos:

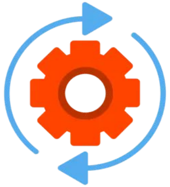
Verificar Trabalhos Anteriores



Definir uma Metodologia de Experimentos

Para atingir este objetivo precisamos:

Verificar Trabalhos Anteriores



Definir uma Metodologia de Experimentos

Analisar os Resultados

Para atingir este objetivo precisamos:

Verificar Trabalhos Anteriores

Definir uma Metodologia de Experimentos

Analisar os Resultados

Definir as conclusões sobre os Resultados

Para atingir este objetivo precisamos:

Verificar Trabalhos Anteriores

Definir uma Metodologia de Experimentos

Analisar os Resultados

Definir as conclusões sobre os Resultados

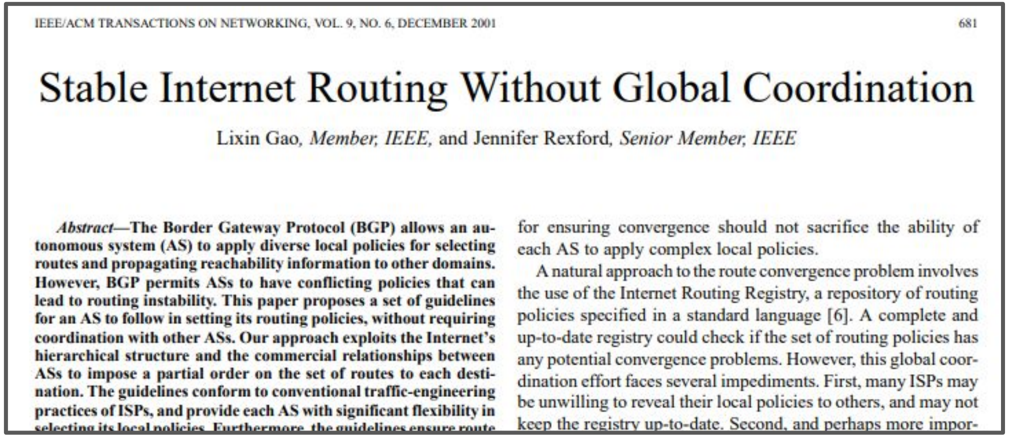
Trabalhos Anteriores sobre Engenharia de Tráfego

Trabalhos Anteriores sobre Engenharia de Tráfego

Modelos existem mas não são seguidos

Trabalhos Anteriores sobre Engenharia de Tráfego

Modelos existem mas não são seguidos



IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 9, NO. 6, DECEMBER 2001 681

Stable Internet Routing Without Global Coordination

Lixin Gao, *Member, IEEE*, and Jennifer Rexford, *Senior Member, IEEE*

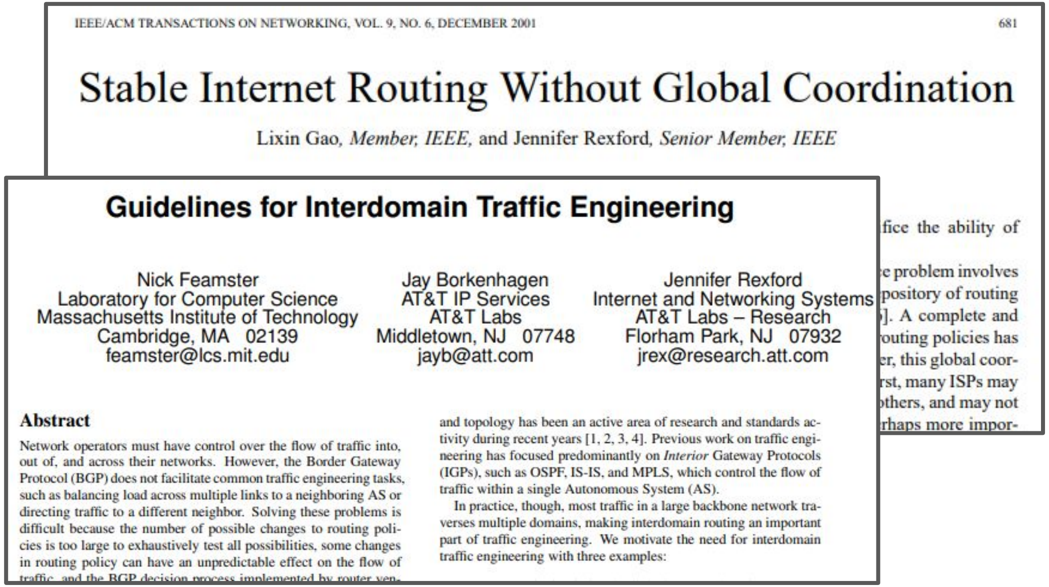
***Abstract*—The Border Gateway Protocol (BGP) allows an autonomous system (AS) to apply diverse local policies for selecting routes and propagating reachability information to other domains. However, BGP permits ASs to have conflicting policies that can lead to routing instability. This paper proposes a set of guidelines for an AS to follow in setting its routing policies, without requiring coordination with other ASs. Our approach exploits the Internet's hierarchical structure and the commercial relationships between ASs to impose a partial order on the set of routes to each destination. The guidelines conform to conventional traffic-engineering practices of ISPs, and provide each AS with significant flexibility in selecting its local policies. Furthermore, the guidelines ensure route**

for ensuring convergence should not sacrifice the ability of each AS to apply complex local policies.

A natural approach to the route convergence problem involves the use of the Internet Routing Registry, a repository of routing policies specified in a standard language [6]. A complete and up-to-date registry could check if the set of routing policies has any potential convergence problems. However, this global coordination effort faces several impediments. First, many ISPs may be unwilling to reveal their local policies to others, and may not keep the registry up-to-date. Second, and perhaps more impor-

Trabalhos Anteriores sobre Engenharia de Tráfego

Modelos existem mas não são seguidos



IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 9, NO. 6, DECEMBER 2001 681

Stable Internet Routing Without Global Coordination

Lixin Gao, *Member, IEEE,* and Jennifer Rexford, *Senior Member, IEEE*

fice the ability of

e problem involves
pository of routing
]. A complete and
outing policies has
er, this global coor-
rst, many ISPs may
others, and may not
rhaps more impor-

Guidelines for Interdomain Traffic Engineering

Nick Feamster
Laboratory for Computer Science
Massachusetts Institute of Technology
Cambridge, MA 02139
feamster@lcs.mit.edu

Jay Borkenhagen
AT&T IP Services
AT&T Labs
Middletown, NJ 07748
jayb@att.com

Jennifer Rexford
Internet and Networking Systems
AT&T Labs – Research
Florham Park, NJ 07932
jrex@research.att.com

Abstract

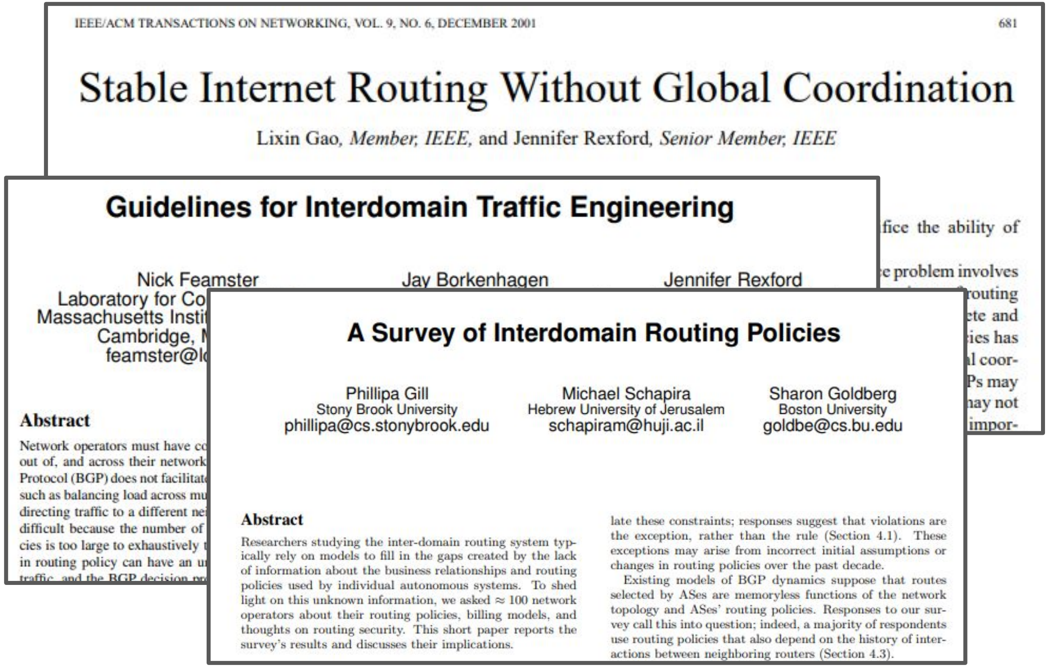
Network operators must have control over the flow of traffic into, out of, and across their networks. However, the Border Gateway Protocol (BGP) does not facilitate common traffic engineering tasks, such as balancing load across multiple links to a neighboring AS or directing traffic to a different neighbor. Solving these problems is difficult because the number of possible changes to routing policies is too large to exhaustively test all possibilities, some changes in routing policy can have an unpredictable effect on the flow of traffic, and the BGP decision process implemented by router ven-

and topology has been an active area of research and standards activity during recent years [1, 2, 3, 4]. Previous work on traffic engineering has focused predominantly on *Interior* Gateway Protocols (IGPs), such as OSPF, IS-IS, and MPLS, which control the flow of traffic within a single Autonomous System (AS).

In practice, though, most traffic in a large backbone network traverses multiple domains, making interdomain routing an important part of traffic engineering. We motivate the need for interdomain traffic engineering with three examples:

Trabalhos Anteriores sobre Engenharia de Tráfego

Modelos existem mas não são seguidos



IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 9, NO. 6, DECEMBER 2001 681

Stable Internet Routing Without Global Coordination

Lixin Gao, *Member, IEEE,* and Jennifer Rexford, *Senior Member, IEEE*

fice the ability of
e problem involves
routing
ete and
ies has
l coor-
Ps may
ay not
impor-

Guidelines for Interdomain Traffic Engineering

Nick Feamster
Laboratory for Co
Massachusetts Instit
Cambridge, M
feamster@l

Jay Borkenhagen

Jennifer Rexford

Abstract

Network operators must have co
out of, and across their network
Protocol (BGP) does not facilitate
such as balancing load across mu
directing traffic to a different ne
difficult because the number of
cies is too large to exhaustively t
in routing policy can have an u
traffic, and the BGP decision pro

A Survey of Interdomain Routing Policies

Phillipa Gill
Stony Brook University
phillipa@cs.stonybrook.edu

Michael Schapira
Hebrew University of Jerusalem
schapiram@huji.ac.il

Sharon Goldberg
Boston University
goldbe@cs.bu.edu

Abstract

Researchers studying the inter-domain routing system typically rely on models to fill in the gaps created by the lack of information about the business relationships and routing policies used by individual autonomous systems. To shed light on this unknown information, we asked ≈ 100 network operators about their routing policies, billing models, and thoughts on routing security. This short paper reports the survey's results and discusses their implications.

late these constraints; responses suggest that violations are the exception, rather than the rule (Section 4.1). These exceptions may arise from incorrect initial assumptions or changes in routing policies over the past decade.

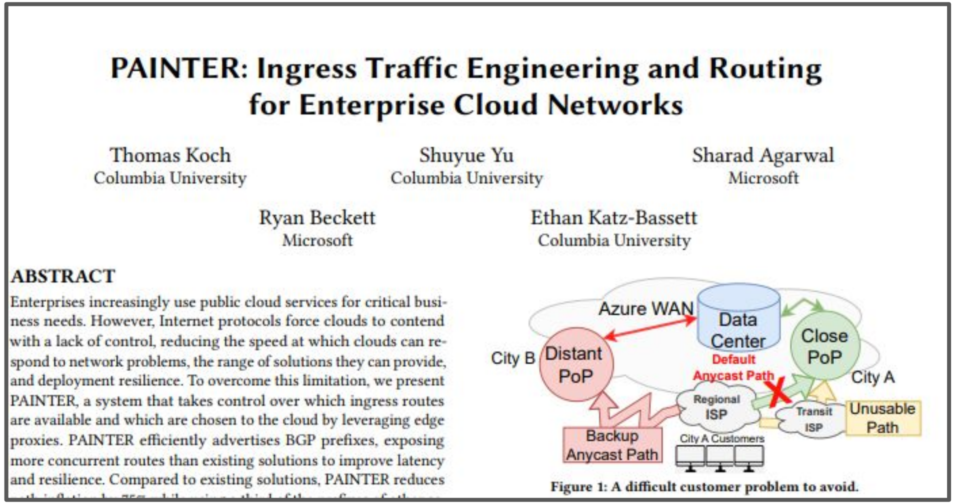
Existing models of BGP dynamics suppose that routes selected by ASes are memoryless functions of the network topology and ASes' routing policies. Responses to our survey call this into question; indeed, a majority of respondents use routing policies that also depend on the history of interactions between neighboring routers (Section 4.3).

Trabalhos Anteriores sobre Engenharia de Tráfego

Ainda existem desafios de roteamento

Trabalhos Anteriores sobre Engenharia de Tráfego

Ainda existem desafios de roteamento



PAINTER: Ingress Traffic Engineering and Routing for Enterprise Cloud Networks

Thomas Koch
Columbia University

Shuyue Yu
Columbia University

Sharad Agarwal
Microsoft

Ryan Beckett
Microsoft

Ethan Katz-Bassett
Columbia University

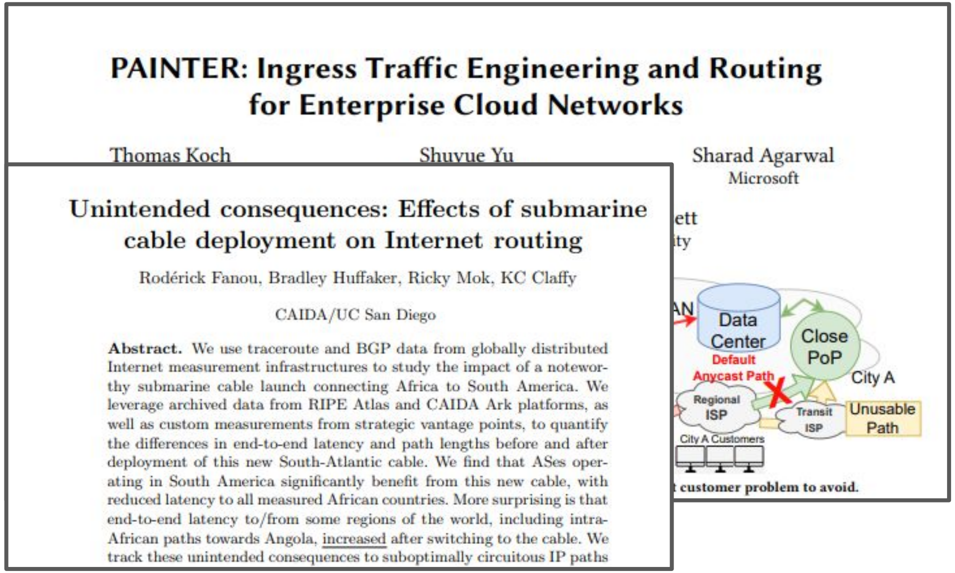
ABSTRACT

Enterprises increasingly use public cloud services for critical business needs. However, Internet protocols force clouds to contend with a lack of control, reducing the speed at which clouds can respond to network problems, the range of solutions they can provide, and deployment resilience. To overcome this limitation, we present PAINTER, a system that takes control over which ingress routes are available and which are chosen to the cloud by leveraging edge proxies. PAINTER efficiently advertises BGP prefixes, exposing more concurrent routes than existing solutions to improve latency and resilience. Compared to existing solutions, PAINTER reduces

Figure 1: A difficult customer problem to avoid.

Trabalhos Anteriores sobre Engenharia de Tráfego

Ainda existem desafios de roteamento



PAINTER: Ingress Traffic Engineering and Routing for Enterprise Cloud Networks

Thomas Koch

Shuyue Yu

Sharad Agarwal
Microsoft

ett

ity

customer problem to avoid.

Unintended consequences: Effects of submarine cable deployment on Internet routing

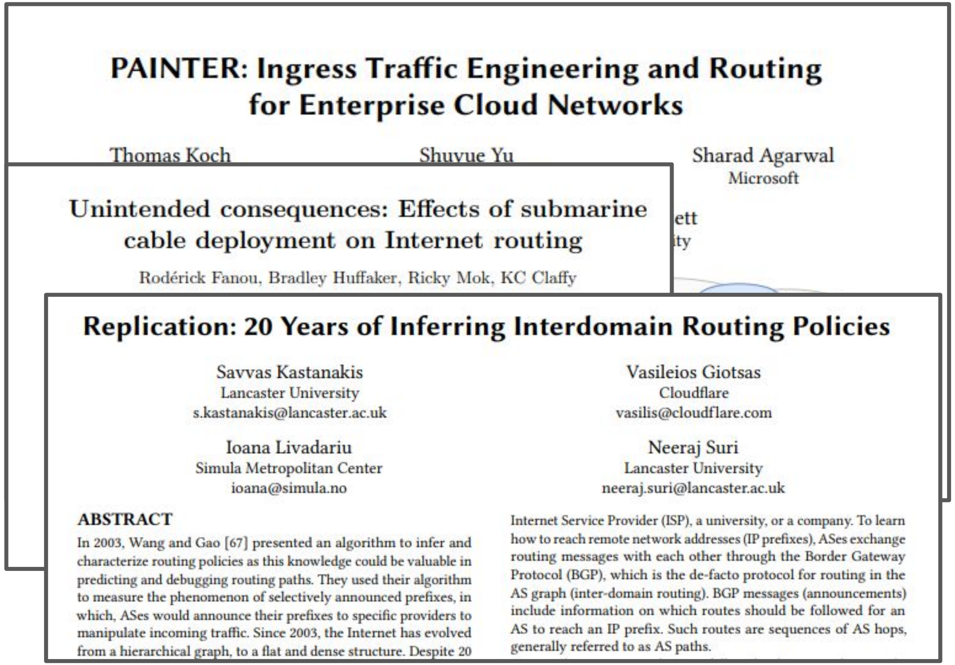
Rodérick Fanou, Bradley Huffaker, Ricky Mok, KC Claffy

CAIDA/UC San Diego

Abstract. We use traceroute and BGP data from globally distributed Internet measurement infrastructures to study the impact of a noteworthy submarine cable launch connecting Africa to South America. We leverage archived data from RIPE Atlas and CAIDA Ark platforms, as well as custom measurements from strategic vantage points, to quantify the differences in end-to-end latency and path lengths before and after deployment of this new South-Atlantic cable. We find that ASes operating in South America significantly benefit from this new cable, with reduced latency to all measured African countries. More surprising is that end-to-end latency to/from some regions of the world, including intra-African paths towards Angola, increased after switching to the cable. We track these unintended consequences to suboptimally circuitous IP paths

Trabalhos Anteriores sobre Engenharia de Tráfego

Ainda existem desafios de roteamento



PAINTER: Ingress Traffic Engineering and Routing for Enterprise Cloud Networks

Thomas Koch
Shuyue Yu
Sharad Agarwal
Microsoft
ett
ity

Unintended consequences: Effects of submarine cable deployment on Internet routing

Rodérick Fanou, Bradley Huffaker, Ricky Mok, KC Claffy

Replication: 20 Years of Inferring Interdomain Routing Policies

Savvas Kastanakis
Lancaster University
s.kastanakis@lancaster.ac.uk

Vasileios Giotsas
Cloudflare
vasilis@cloudflare.com

Ioana Livadariu
Simula Metropolitan Center
ioana@simula.no

Neeraj Suri
Lancaster University
neeraj.suri@lancaster.ac.uk

ABSTRACT

In 2003, Wang and Gao [67] presented an algorithm to infer and characterize routing policies as this knowledge could be valuable in predicting and debugging routing paths. They used their algorithm to measure the phenomenon of selectively announced prefixes, in which, ASes would announce their prefixes to specific providers to manipulate incoming traffic. Since 2003, the Internet has evolved from a hierarchical graph, to a flat and dense structure. Despite 20

Internet Service Provider (ISP), a university, or a company. To learn how to reach remote network addresses (IP prefixes), ASes exchange routing messages with each other through the Border Gateway Protocol (BGP), which is the de-facto protocol for routing in the AS graph (inter-domain routing). BGP messages (announcements) include information on which routes should be followed for an AS to reach an IP prefix. Such routes are sequences of AS hops, generally referred to as AS paths.

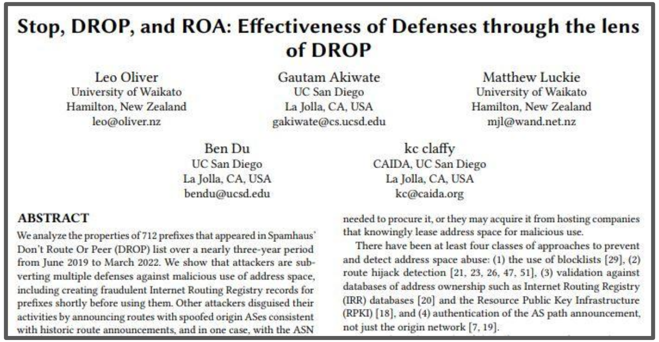
Sobre Eventos de Sequestro de Prefixo

Sobre Eventos de Sequestro de Prefixo

Ferramentas de mitigação possuem falhas

Sobre Eventos de Sequestro de Prefixo

Ferramentas de mitigação possuem falhas



Stop, DROP, and ROA: Effectiveness of Defenses through the lens of DROP

Leo Oliver
University of Waikato
Hamilton, New Zealand
leo@oliver.nz

Gautam Akiwate
UC San Diego
La Jolla, CA, USA
gakiwate@cs.ucsd.edu

Matthew Luckie
University of Waikato
Hamilton, New Zealand
mjl@wand.net.nz

Ben Du
UC San Diego
La Jolla, CA, USA
bendu@ucsd.edu

kc claffy
CAIDA, UC San Diego
La Jolla, CA, USA
kc@caida.org

ABSTRACT

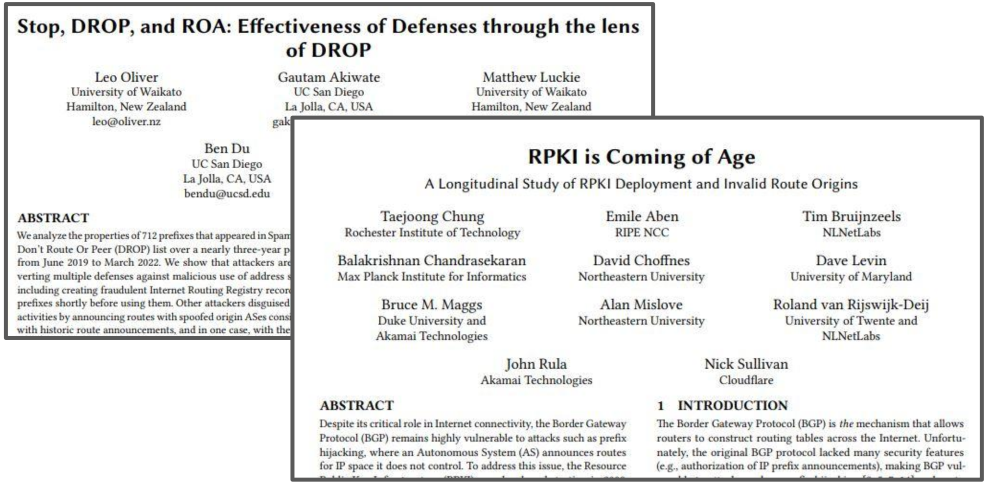
We analyze the properties of 712 prefixes that appeared in Spamhaus' Don't Route Or Peer (DROP) list over a nearly three-year period from June 2019 to March 2022. We show that attackers are subverting multiple defenses against malicious use of address space, including creating fraudulent Internet Routing Registry records for prefixes shortly before using them. Other attackers disguised their activities by announcing routes with spoofed origin ASes consistent with historic route announcements, and in one case, with the ASN

needed to procure it, or they may acquire it from hosting companies that knowingly lease address space for malicious use.

There have been at least four classes of approaches to prevent and detect address space abuse: (1) the use of blocklists [29], (2) route hijack detection [21, 23, 26, 47, 51], (3) validation against databases of address ownership such as Internet Routing Registry (IRR) databases [20] and the Resource Public Key Infrastructure (RPKI) [18], and (4) authentication of the AS path announcement, not just the origin network [7, 19].

Sobre Eventos de Sequestro de Prefixo

Ferramentas de mitigação possuem falhas



Stop, DROP, and ROA: Effectiveness of Defenses through the lens of DROP

Leo Oliver
University of Waikato
Hamilton, New Zealand
leo@oliver.nz

Gautam Akiwate
UC San Diego
La Jolla, CA, USA
gak

Matthew Luckie
University of Waikato
Hamilton, New Zealand

Ben Du
UC San Diego
La Jolla, CA, USA
bendu@ucsd.edu

ABSTRACT

We analyze the properties of 712 prefixes that appeared in Spam
Don't Route Or Peer (DROP) list over a nearly three-year p
from June 2019 to March 2022. We show that attackers are
verting multiple defenses against malicious use of address s
including creating fraudulent Internet Routing Registry recor
prefixes shortly before using them. Other attackers disguised
activities by announcing routes with spoofed origin ASes consi
with historic route announcements, and in one case, with the

RPKI is Coming of Age

A Longitudinal Study of RPKI Deployment and Invalid Route Origins

Taejoong Chung
Rochester Institute of Technology

Emile Aben
RIPE NCC

Tim Bruijnzeels
NLNetLabs

Balakrishnan Chandrasekaran
Max Planck Institute for Informatics

David Choffnes
Northeastern University

Dave Levin
University of Maryland

Bruce M. Maggs
Duke University and
Akamai Technologies

Alan Mislove
Northeastern University

Roland van Rijswijk-Deij
University of Twente and
NLNetLabs

John Rula
Akamai Technologies

Nick Sullivan
Cloudflare

ABSTRACT

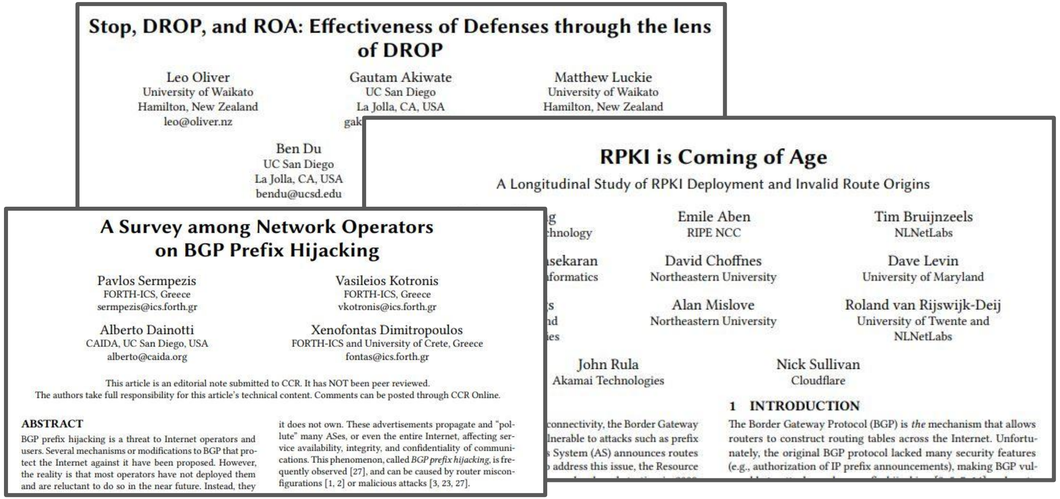
Despite its critical role in Internet connectivity, the Border Gateway Protocol (BGP) remains highly vulnerable to attacks such as prefix hijacking, where an Autonomous System (AS) announces routes for IP space it does not control. To address this issue, the Resource

1 INTRODUCTION

The Border Gateway Protocol (BGP) is *the* mechanism that allows routers to construct routing tables across the Internet. Unfortunately, the original BGP protocol lacked many security features (e.g., authorization of IP prefix announcements), making BGP vul-

Sobre Eventos de Sequestro de Prefixo

Ferramentas de mitigação possuem falhas



Stop, DROP, and ROA: Effectiveness of Defenses through the lens of DROP

Leo Oliver
University of Waikato
Hamilton, New Zealand
leo@oliver.nz

Gautam Akiwate
UC San Diego
La Jolla, CA, USA
gak

Matthew Luckie
University of Waikato
Hamilton, New Zealand

Ben Du
UC San Diego
La Jolla, CA, USA
bendu@ucsd.edu

RPKI is Coming of Age

A Longitudinal Study of RPKI Deployment and Invalid Route Origins

g
chnology

Emile Aben
RIPE NCC

Tim Bruijnzeels
NLNetLabs

sekaran
formatics

David Choffnes
Northeastern University

Dave Levin
University of Maryland

s
nd
ies

Alan Mislove
Northeastern University

Roland van Rijswijk-Deij
University of Twente and
NLNetLabs

John Rula
Akamai Technologies

Nick Sullivan
Cloudflare

connectivity, the Border Gateway lnerable to attacks such as prefix s System (AS) announces routes address this issue, the Resource

1 INTRODUCTION

The Border Gateway Protocol (BGP) is *the* mechanism that allows routers to construct routing tables across the Internet. Unfortunately, the original BGP protocol lacked many security features (e.g., authorization of IP prefix announcements), making BGP vul-

A Survey among Network Operators on BGP Prefix Hijacking

Pavlos Sermpezis
FORTH-ICS, Greece
sermpezis@ics.forth.gr

Vasileios Kotronis
FORTH-ICS, Greece
vkotronis@ics.forth.gr

Alberto Dainotti
CAIDA, UC San Diego, USA
alberto@caida.org

Xenofontas Dimitropoulos
FORTH-ICS and University of Crete, Greece
fontas@ics.forth.gr

This article is an editorial note submitted to CCR. It has NOT been peer reviewed.
The authors take full responsibility for this article's technical content. Comments can be posted through CCR Online.

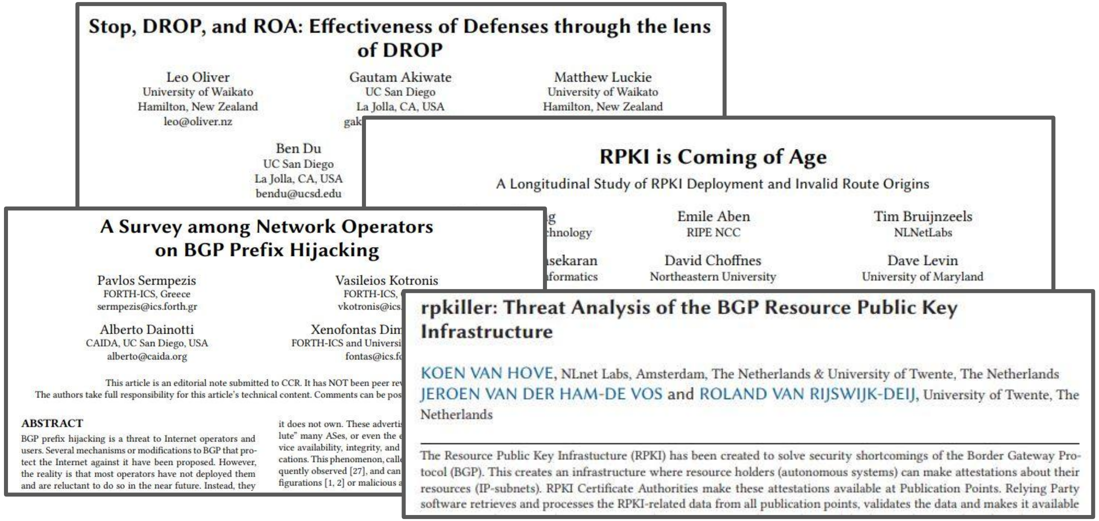
ABSTRACT

BGP prefix hijacking is a threat to Internet operators and users. Several mechanisms or modifications to BGP that protect the Internet against it have been proposed. However, the reality is that most operators have not deployed them and are reluctant to do so in the near future. Instead, they

it does not own. These advertisements propagate and "pollute" many ASes, or even the entire Internet, affecting service availability, integrity, and confidentiality of communications. This phenomenon, called *BGP prefix hijacking*, is frequently observed [27], and can be caused by router misconfigurations [1, 2] or malicious attacks [3, 23, 27].

Sobre Eventos de Sequestro de Prefixo

Ferramentas de mitigação possuem falhas



Stop, DROP, and ROA: Effectiveness of Defenses through the lens of DROP

Leo Oliver
University of Waikato
Hamilton, New Zealand
leo@oliver.nz

Gautam Akiwate
UC San Diego
La Jolla, CA, USA
gak

Matthew Luckie
University of Waikato
Hamilton, New Zealand

Ben Du
UC San Diego
La Jolla, CA, USA
bendu@ucsd.edu

RPKI is Coming of Age

A Longitudinal Study of RPKI Deployment and Invalid Route Origins

g
chnology

Emile Aben
RIPE NCC

Tim Bruijnzeels
NLNetLabs

sekaran
formatics

David Choffnes
Northeastern University

Dave Levin
University of Maryland

A Survey among Network Operators on BGP Prefix Hijacking

Pavlos Sermpezis
FORTH-ICS, Greece
sermpezis@ics.forth.gr

Vasileios Kotronis
FORTH-ICS,
vkotronis@ics.

Alberto Dainotti
CAIDA, UC San Diego, USA
alberto@caida.org

Xenofontas Dim
FORTH-ICS and Universi
fontas@ics.f

This article is an editorial note submitted to CCR. It has NOT been peer rev
The authors take full responsibility for this article's technical content. Comments can be pos

ABSTRACT

BGP prefix hijacking is a threat to Internet operators and users. Several mechanisms or modifications to BGP that protect the Internet against it have been proposed. However, the reality is that most operators have not deployed them and are reluctant to do so in the near future. Instead, they

it does not own. These advertis
lute" many ASes, or even the e
vice availability, integrity, and
cations. This phenomenon, calle
quently observed [27], and can
figurations [1, 2] or malicious a

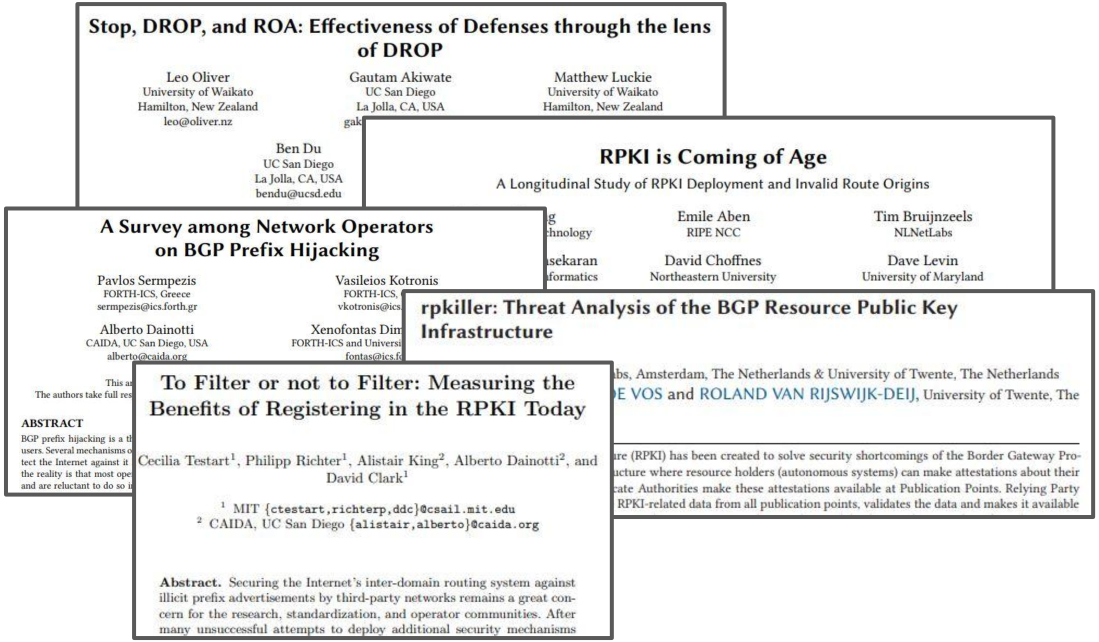
rpkiller: Threat Analysis of the BGP Resource Public Key Infrastructure

KOEN VAN HOVE, NLnet Labs, Amsterdam, The Netherlands & University of Twente, The Netherlands
JEROEN VAN DER HAM-DE VOS and ROLAND VAN RIJSWIJK-DEIJ, University of Twente, The Netherlands

The Resource Public Key Infrastucture (RPKI) has been created to solve security shortcomings of the Border Gateway Protocol (BGP). This creates an infrastructure where resource holders (autonomous systems) can make attestations about their resources (IP-subnets). RPKI Certificate Authorities make these attestations available at Publication Points. Relying Party software retrieves and processes the RPKI-related data from all publication points, validates the data and makes it available

Sobre Eventos de Sequestro de Prefixo

Ferramentas de mitigação possuem falhas



Stop, DROP, and ROA: Effectiveness of Defenses through the lens of DROP

Leo Oliver
University of Waikato
Hamilton, New Zealand
leo@oliver.nz

Gautam Akiwate
UC San Diego
La Jolla, CA, USA
gak

Matthew Luckie
University of Waikato
Hamilton, New Zealand

Ben Du
UC San Diego
La Jolla, CA, USA
bendu@ucsd.edu

RPKI is Coming of Age

A Longitudinal Study of RPKI Deployment and Invalid Route Origins

g
chnology

Emile Aben
RIPE NCC

Tim Bruijnzeels
NLNetLabs

asekaran
formatics

David Choffnes
Northeastern University

Dave Levin
University of Maryland

A Survey among Network Operators on BGP Prefix Hijacking

Pavlos Sermpezis
FORTH-ICS, Greece
sermpezis@ics.forth.gr

Vasileios Kotronis
FORTH-ICS,
vkotronis@ics

Alberto Dainotti
CAIDA, UC San Diego, USA
alberto@caida.org

Xenofontas Dim
FORTH-ICS and Universi
fontas@ics.fo

This ar
The authors take full res

ABSTRACT

BGP prefix hijacking is a th
users. Several mechanisms o
tect the Internet against it
the reality is that most ope
and are reluctant to do so i

rpkiller: Threat Analysis of the BGP Resource Public Key Infrastructure

bs, Amsterdam, The Netherlands & University of Twente, The Netherlands
E VOS and ROLAND VAN RIJSWIJK-DEIJ, University of Twente, The

re (RPKI) has been created to solve security shortcomings of the Border Gateway Pro-
ucture where resource holders (autonomous systems) can make attestations about their
cate Authorities make these attestations available at Publication Points. Relying Party
RPKI-related data from all publication points, validates the data and makes it available

To Filter or not to Filter: Measuring the Benefits of Registering in the RPKI Today

Cecilia Testart[1], Philipp Richter[1], Alistair King[2], Alberto Dainotti[2], and David Clark[1]

[1] MIT {ctestart,richterp,ddc}@csail.mit.edu
[2] CAIDA, UC San Diego {alistair,alberto}@caida.org

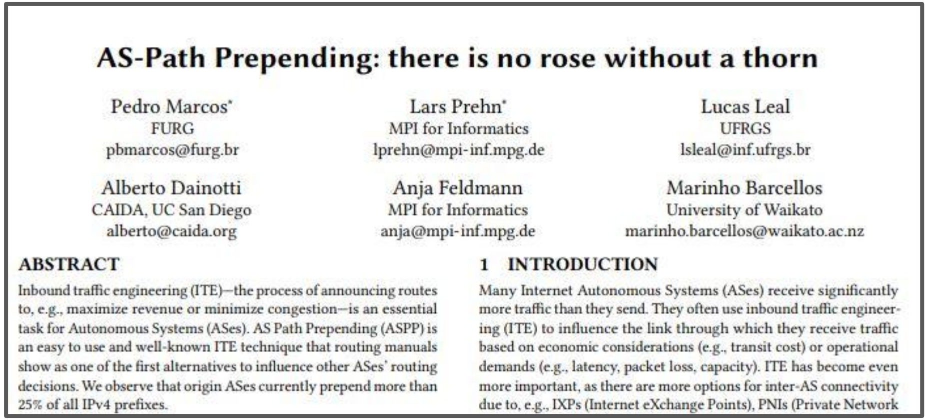
Abstract. Securing the Internet's inter-domain routing system against illicit prefix advertisements by third-party networks remains a great concern for the research, standardization, and operator communities. After many unsuccessful attempts to deploy additional security mechanisms

Sobre Eventos de Sequestro de Prefixo

Lacunas no entendimento do impacto

Sobre Eventos de Sequestro de Prefixo

Lacunas no entendimento do impacto



AS-Path Prepending: there is no rose without a thorn

Pedro Marcos*
FURG
pbmarcos@furg.br

Lars Prehn*
MPI for Informatics
lprehn@mpi-inf.mpg.de

Lucas Leal
UFRGS
lsleal@inf.ufrgs.br

Alberto Dainotti
CAIDA, UC San Diego
alberto@caida.org

Anja Feldmann
MPI for Informatics
anja@mpi-inf.mpg.de

Marinho Barcellos
University of Waikato
marinho.barcellos@waikato.ac.nz

ABSTRACT

Inbound traffic engineering (ITE)—the process of announcing routes to, e.g., maximize revenue or minimize congestion—is an essential task for Autonomous Systems (ASes). AS Path Prepending (ASPP) is an easy to use and well-known ITE technique that routing manuals show as one of the first alternatives to influence other ASes' routing decisions. We observe that origin ASes currently prepend more than 25% of all IPv4 prefixes.

1 INTRODUCTION

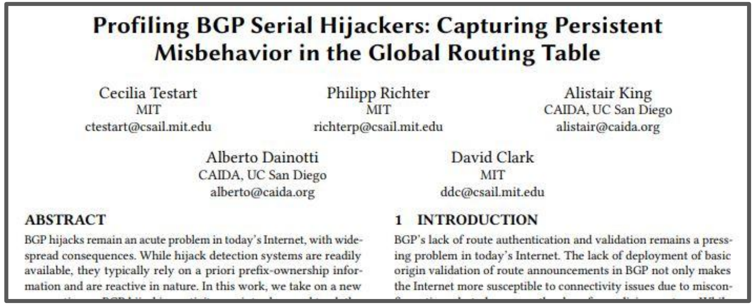
Many Internet Autonomous Systems (ASes) receive significantly more traffic than they send. They often use inbound traffic engineering (ITE) to influence the link through which they receive traffic based on economic considerations (e.g., transit cost) or operational demands (e.g., latency, packet loss, capacity). ITE has become even more important, as there are more options for inter-AS connectivity due to, e.g., IXPs (Internet eXchange Points), PNIs (Private Network

Sobre Eventos de Sequestro de Prefixo

Sequestros
Acontecem
diariamente

Sobre Eventos de Sequestro de Prefixo

Sequestros Acontecem diariamente



Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table

Cecilia Testart
MIT
ctestart@csail.mit.edu

Philipp Richter
MIT
richterp@csail.mit.edu

Alistair King
CAIDA, UC San Diego
alistair@caida.org

Alberto Dainotti
CAIDA, UC San Diego
alberto@caida.org

David Clark
MIT
ddc@csail.mit.edu

ABSTRACT

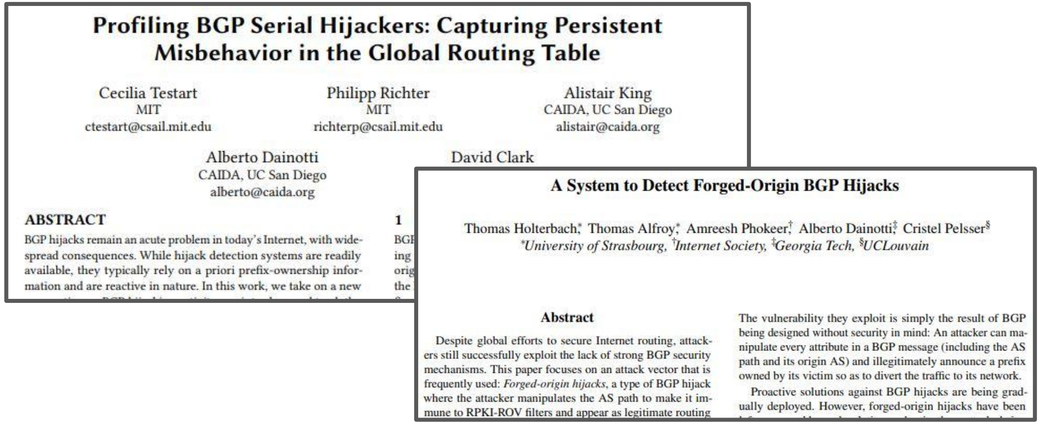
BGP hijacks remain an acute problem in today's Internet, with widespread consequences. While hijack detection systems are readily available, they typically rely on a priori prefix-ownership information and are reactive in nature. In this work, we take on a new

1 INTRODUCTION

BGP's lack of route authentication and validation remains a pressing problem in today's Internet. The lack of deployment of basic origin validation of route announcements in BGP not only makes the Internet more susceptible to connectivity issues due to miscon-

Sobre Eventos de Sequestro de Prefixo

Sequestros Acontecem diariamente



Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table

Cecilia Testart
MIT
ctestart@csail.mit.edu

Philipp Richter
MIT
richterp@csail.mit.edu

Alistair King
CAIDA, UC San Diego
alistair@caida.org

Alberto Dainotti
CAIDA, UC San Diego
alberto@caida.org

David Clark

ABSTRACT

BGP hijacks remain an acute problem in today's Internet, with widespread consequences. While hijack detection systems are readily available, they typically rely on a priori prefix-ownership information and are reactive in nature. In this work, we take on a new

A System to Detect Forged-Origin BGP Hijacks

Thomas Holterbach[*], Thomas Alfroy[*], Amreesh Phokeer[†], Alberto Dainotti[‡], Cristel Pelsser[§]
[*]University of Strasbourg, [†]Internet Society, [‡]Georgia Tech, [§]UCLouvain

Abstract

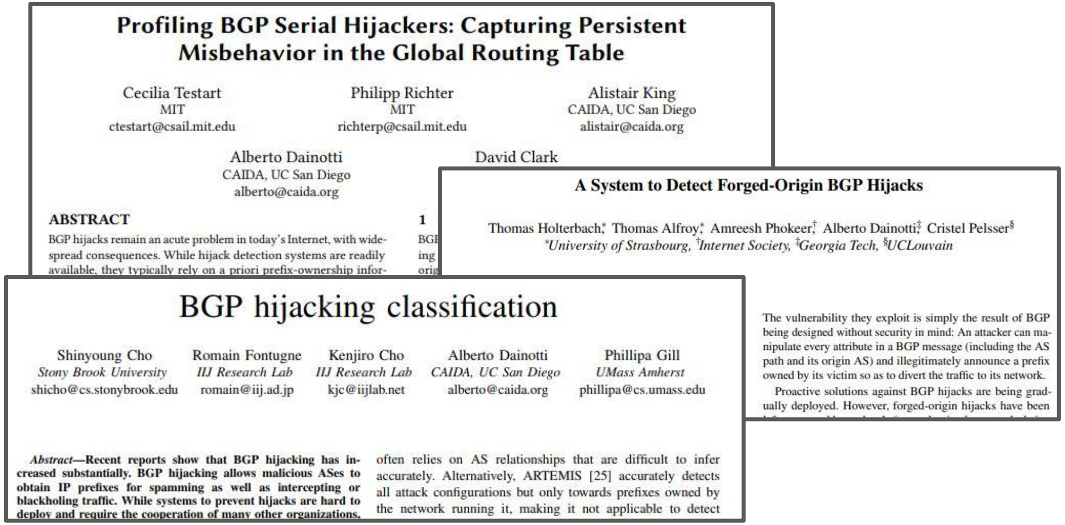
Despite global efforts to secure Internet routing, attackers still successfully exploit the lack of strong BGP security mechanisms. This paper focuses on an attack vector that is frequently used: *Forged-origin hijacks*, a type of BGP hijack where the attacker manipulates the AS path to make it immune to RPKI-ROV filters and appear as legitimate routing

The vulnerability they exploit is simply the result of BGP being designed without security in mind: An attacker can manipulate every attribute in a BGP message (including the AS path and its origin AS) and illegitimately announce a prefix owned by its victim so as to divert the traffic to its network.

Proactive solutions against BGP hijacks are being gradually deployed. However, forged-origin hijacks have been

Sobre Eventos de Sequestro de Prefixo

Sequestros Acontecem diariamente



Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table

Cecilia Testart
MIT
ctestart@csail.mit.edu

Philipp Richter
MIT
richterp@csail.mit.edu

Alistair King
CAIDA, UC San Diego
alistair@caida.org

Alberto Dainotti
CAIDA, UC San Diego
alberto@caida.org

David Clark

ABSTRACT

BGP hijacks remain an acute problem in today's Internet, with widespread consequences. While hijack detection systems are readily available, they typically rely on a priori prefix-ownership infor-

1

BGI
ing
orig

A System to Detect Forged-Origin BGP Hijacks

Thomas Holterbach[*], Thomas Alfroy[*], Amreesh Phokeer[†], Alberto Dainotti[‡], Cristel Pelsser[§]
[*]University of Strasbourg, [†]Internet Society, [‡]Georgia Tech, [§]UCLouvain

The vulnerability they exploit is simply the result of BGP being designed without security in mind: An attacker can manipulate every attribute in a BGP message (including the AS path and its origin AS) and illegitimately announce a prefix owned by its victim so as to divert the traffic to its network.

Proactive solutions against BGP hijacks are being gradually deployed. However, forged-origin hijacks have been

BGP hijacking classification

Shinyoung Cho
Stony Brook University
shicho@cs.stonybrook.edu

Romain Fontugne
IIJ Research Lab
romain@iij.ad.jp

Kenjiro Cho
IIJ Research Lab
kjc@iijlab.net

Alberto Dainotti
CAIDA, UC San Diego
alberto@caida.org

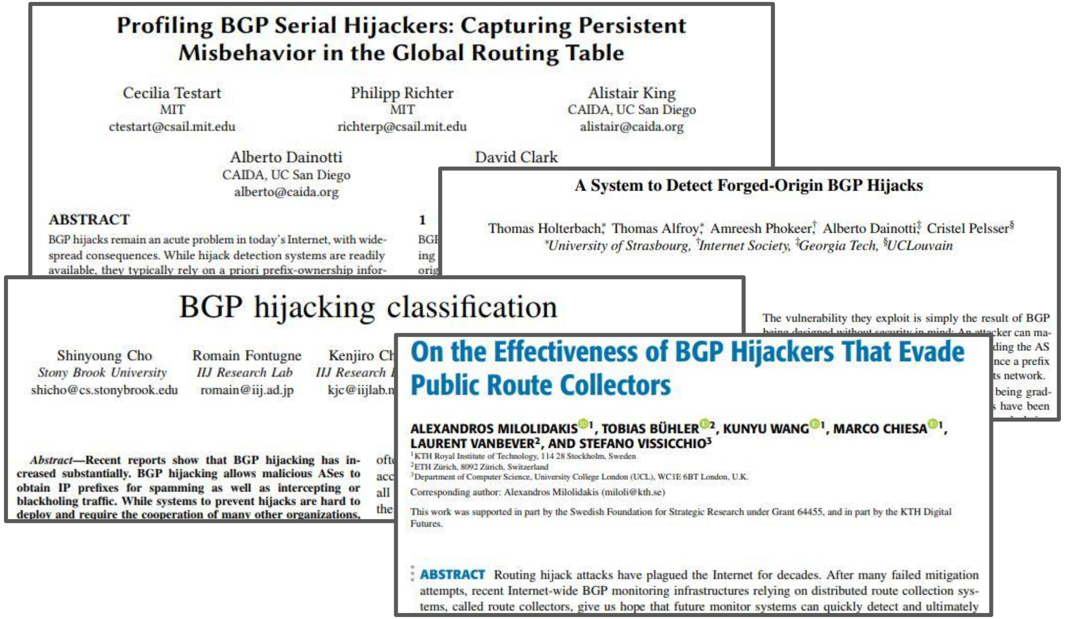
Phillipa Gill
UMass Amherst
phillipa@cs.umass.edu

Abstract—**Recent reports show that BGP hijacking has increased substantially. BGP hijacking allows malicious ASes to obtain IP prefixes for spamming as well as intercepting or blackholing traffic. While systems to prevent hijacks are hard to deploy and require the cooperation of many other organizations,**

often relies on AS relationships that are difficult to infer accurately. Alternatively, ARTEMIS [25] accurately detects all attack configurations but only towards prefixes owned by the network running it, making it not applicable to detect

Sobre Eventos de Sequestro de Prefixo

Sequestros
Acontecem
diariamente



Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table

Cecilia Testart
MIT
ctestart@csail.mit.edu

Philipp Richter
MIT
richterp@csail.mit.edu

Alistair King
CAIDA, UC San Diego
alistair@caida.org

Alberto Dainotti
CAIDA, UC San Diego
alberto@caida.org

David Clark

ABSTRACT

BGP hijacks remain an acute problem in today's Internet, with widespread consequences. While hijack detection systems are readily available, they typically rely on a priori prefix-ownership infor-

1
BGI
ing
orig

A System to Detect Forged-Origin BGP Hijacks

Thomas Holterbach, Thomas Alfroy, Amreesh Phokeer, Alberto Dainotti, Cristel Pelsser
University of Strasbourg, Internet Society, Georgia Tech, UCLouvain

The vulnerability they exploit is simply the result of BGP being designed without security in mind: An attacker can ma- … ding the AS … nce a prefix … ts network. … being grad- … have been

BGP hijacking classification

Shinyoung Cho
Stony Brook University
shicho@cs.stonybrook.edu

Romain Fontugne
IIJ Research Lab
romain@iij.ad.jp

Kenjiro Ch
IIJ Research
kjc@iijlab.n

Abstract—Recent reports show that BGP hijacking has increased substantially. BGP hijacking allows malicious ASes to obtain IP prefixes for spamming as well as intercepting or blackholing traffic. While systems to prevent hijacks are hard to deploy and require the cooperation of many other organizations,

oft
acc
all
the

On the Effectiveness of BGP Hijackers That Evade Public Route Collectors

ALEXANDROS MILOLIDAKIS[1], TOBIAS BÜHLER[2], KUNYU WANG[1], MARCO CHIESA[1], LAURENT VANBEVER[2], AND STEFANO VISSICCHIO[3]
[1]KTH Royal Institute of Technology, 114 28 Stockholm, Sweden
[2]ETH Zürich, 8092 Zürich, Switzerland
[3]Department of Computer Science, University College London (UCL), WC1E 6BT London, U.K.

Corresponding author: Alexandros Milolidakis (miloli@kth.se)

This work was supported in part by the Swedish Foundation for Strategic Research under Grant 64455, and in part by the KTH Digital Futures.

ABSTRACT Routing hijack attacks have plagued the Internet for decades. After many failed mitigation attempts, recent Internet-wide BGP monitoring infrastructures relying on distributed route collection systems, called route collectors, give us hope that future monitor systems can quickly detect and ultimately

Sobre Eventos de Sequestro de Prefixo

Modelos existem mas não são seguidos

Ainda existem desafios de roteamento

Ferramentas de mitigação possuem falhas

Lacunas no entendimento do impacto

Sequestros Acontecem diariamente

Verificar Trabalhos Anteriores

Definir uma Metodologia de Experimentos

Analisar os Resultados

Definir as conclusões sobre os Resultados

Para estudar o impacto de segurança da Engenharia de Tráfego Iremos:

Para estudar o impacto de segurança da Engenharia de Tráfego Iremos:

Definir uma metodologia de experimentos

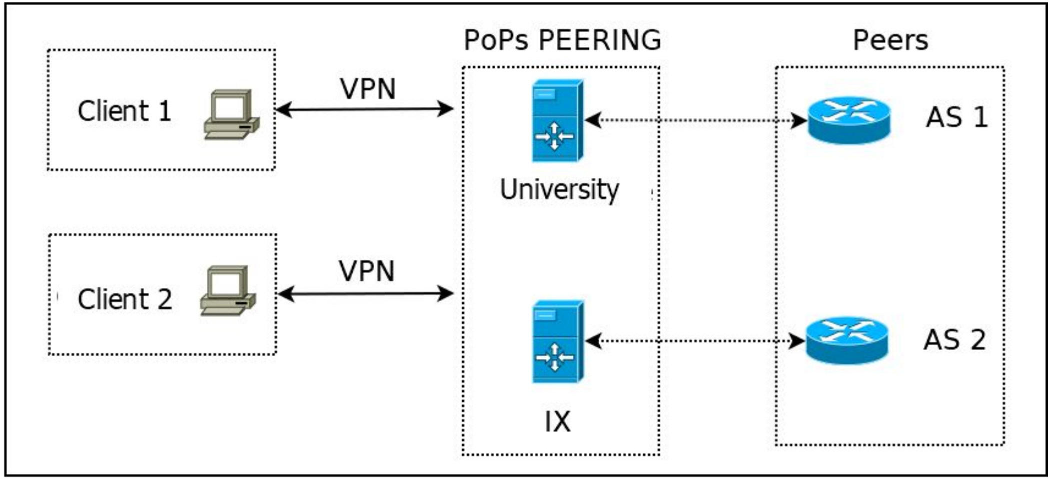
Para estudar o impacto de segurança da Engenharia de Tráfego Iremos:

Definir uma metodologia de experimentos

PEERING
Research Testbed

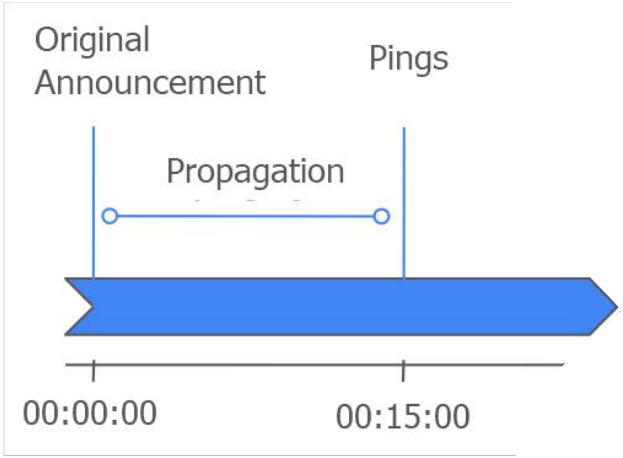
Utilizar o PEERING para realizar estes experimentos

PEERING permite que anúncios BGP sejam realizados na Internet



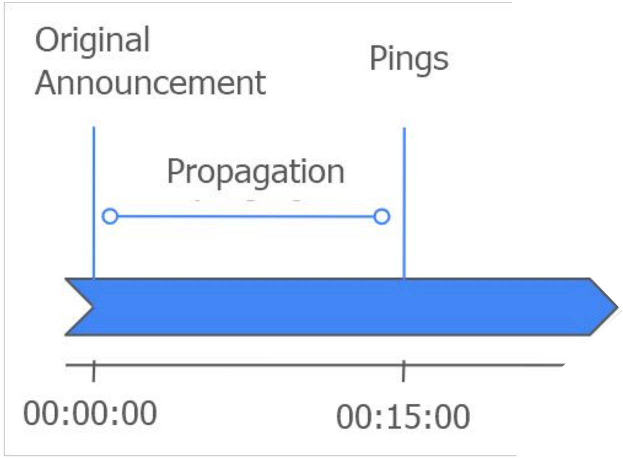
- Diferentes pontos de presença/muxes em múltiplas localidades
- Possível instanciar diferentes ASes

Sobre o Experimento



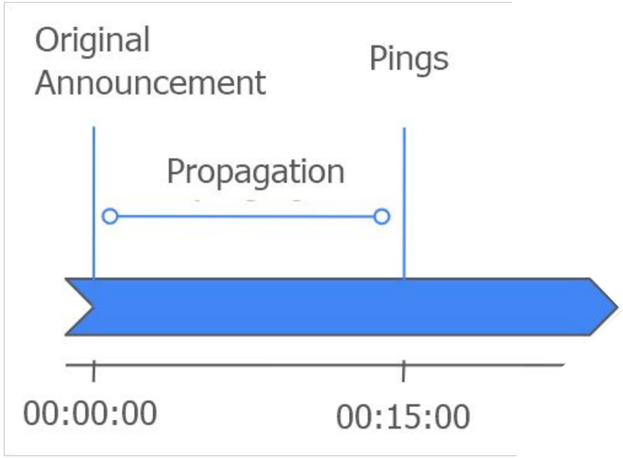
- Vítima anuncia um prefixo

Sobre o Experimento



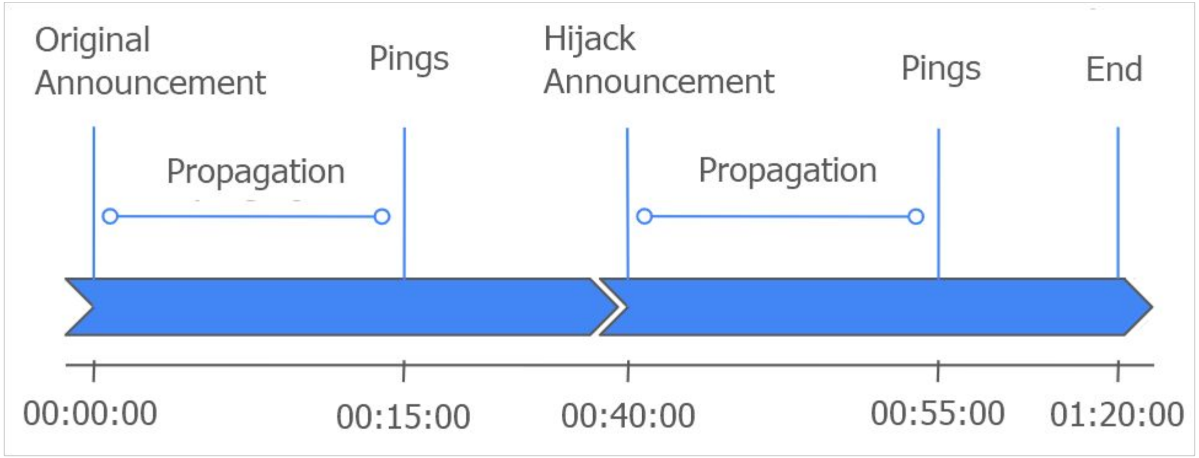
- Vítima anuncia um prefixo
- Comportamento do Anúncio Original

Sobre o Experimento



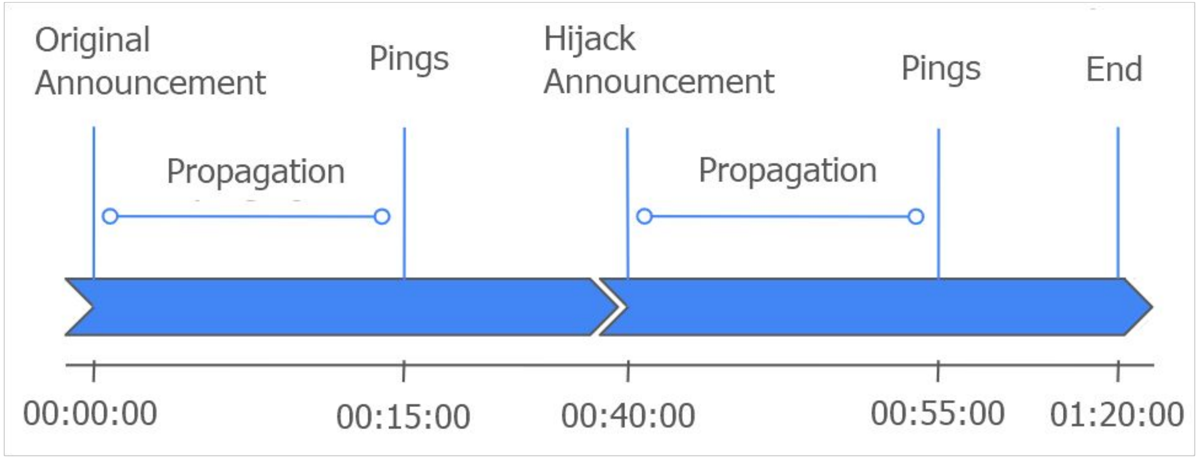
- Vítima anuncia um prefixo
- Comportamento do Anúncio Original
- Define o Baseline para aquele AS

Sobre o Experimento



- Atacante inicia o Sequestro

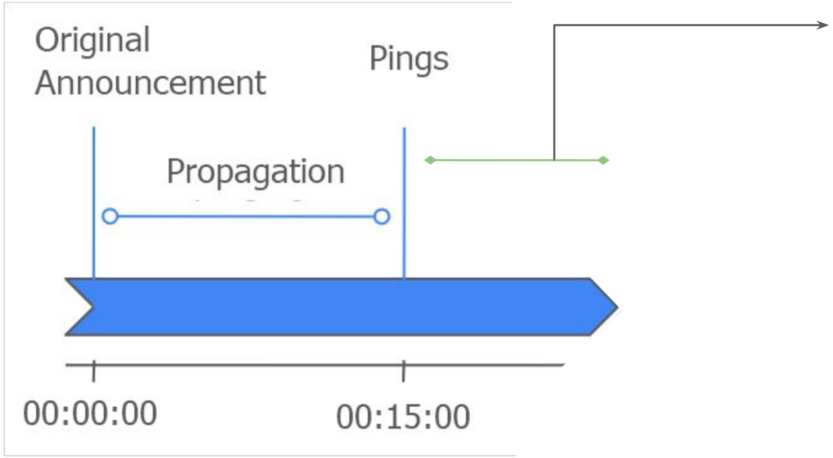
Sobre o Experimento



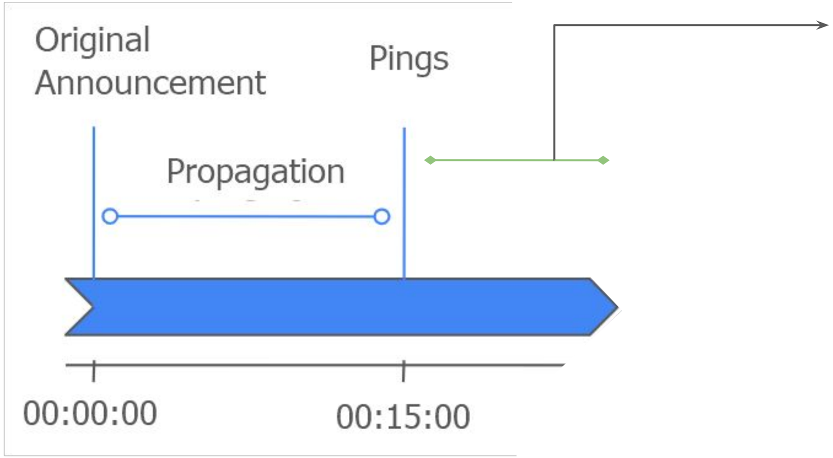
- Atacante inicia o Sequestro
- Define o Impacto do sequestro

Iremos variar, a cada rodada, o uso de técnicas, localização dos ASes e conectividade

Coleta de Dados em Ambos Planos

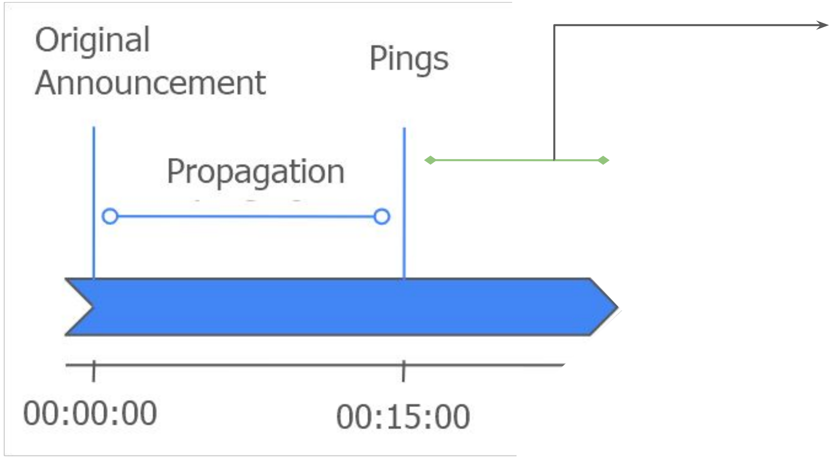


Coleta de Dados em Ambos Planos



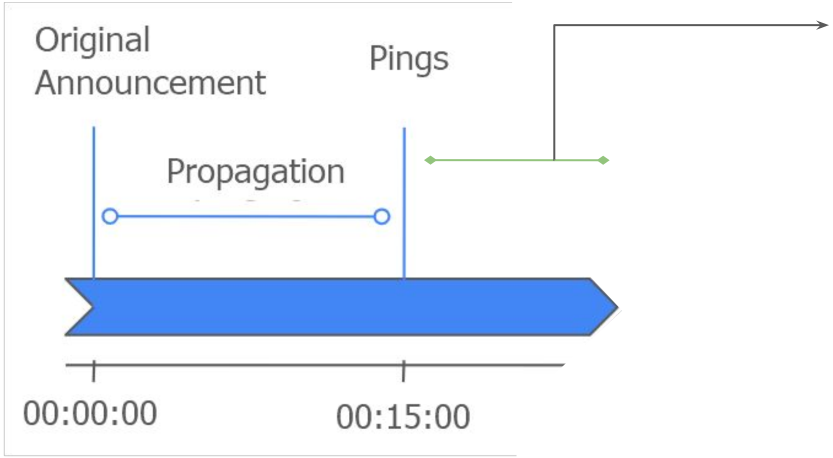
- Coleta no Plano de Dados

Coleta de Dados em Ambos Planos



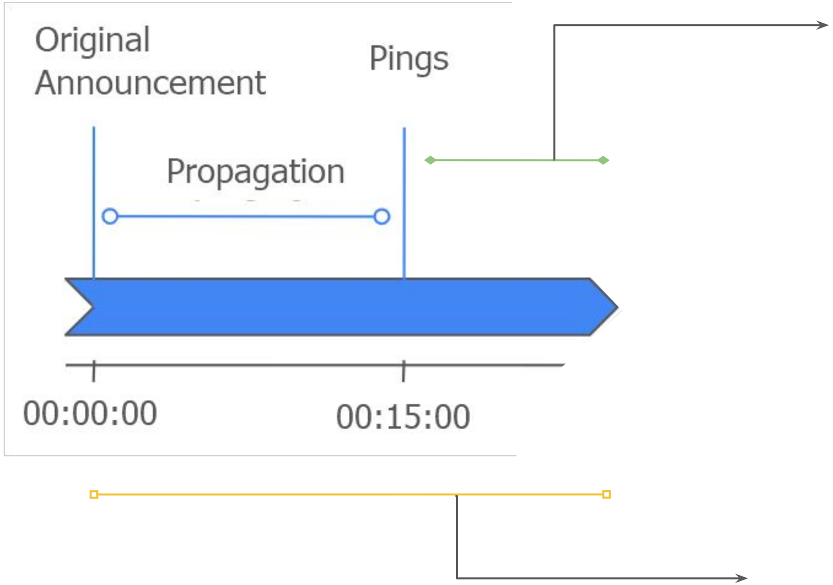
- Coleta no Plano de Dados
- Pings para alvos de uma Hitlist

Coleta de Dados em Ambos Planos



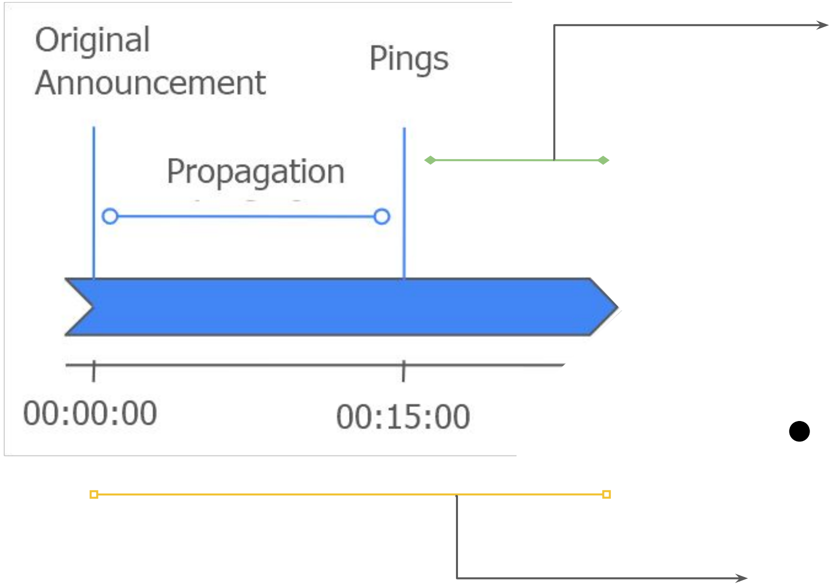
- Coleta no Plano de Dados
- Pings para alvos de uma Hitlist
- Interface e Mac definem por qual AS foi recebida a resposta

Coleta de Dados em Ambos Planos



- Coleta no Plano de Dados
- Pings para alvos de uma Hitlist
- Interface e Mac definem por qual AS foi recebida a resposta

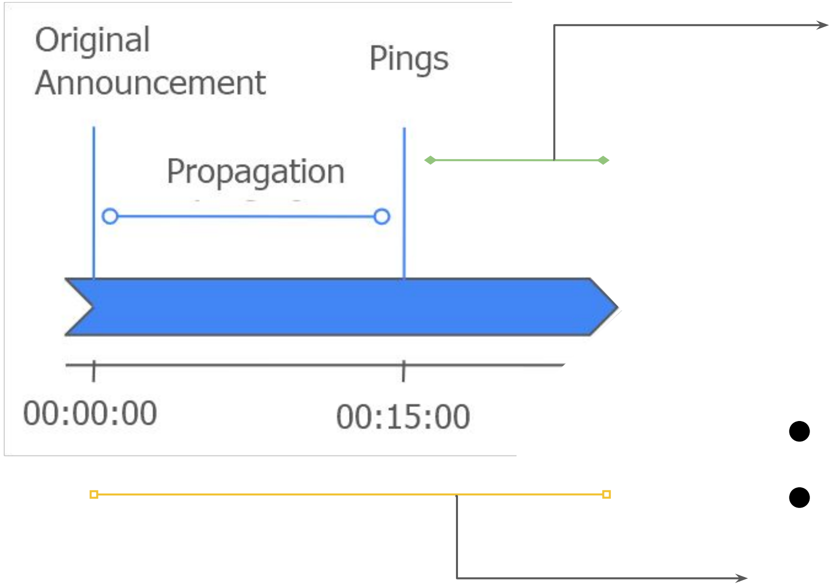
Coleta de Dados em Ambos Planos



- Coleta no Plano de Dados
- Pings para alvos de uma Hitlist
- Interface e Mac definem por qual AS foi recebida a resposta

- Coleta no Plano de Controle

Coleta de Dados em Ambos Planos

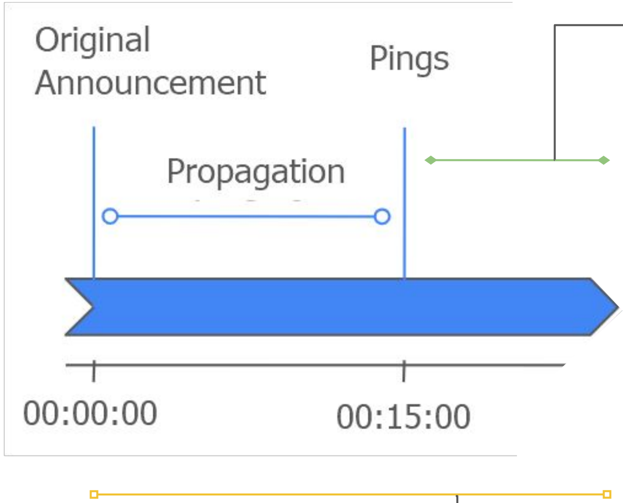


- Coleta no Plano de Dados
- Pings para alvos de uma Hitlist
- Interface e Mac definem por qual AS foi recebida a resposta

- Coleta no Plano de Controle
- Monitores do RIS Live

RIPE NCC

Coleta de Dados em Ambos Planos

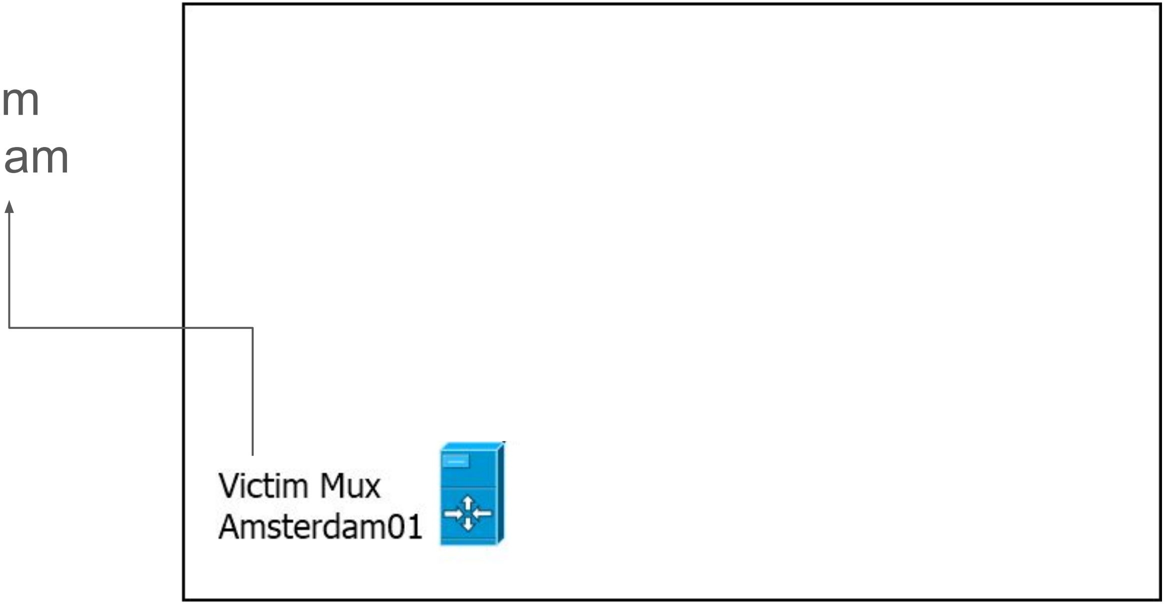


- Coleta no Plano de Dados
- Pings para alvos de uma Hitlist
- Interface e Mac definem por qual AS foi recebida a resposta

- Coleta no Plano de Controle
- Monitores do RIS Live
- Updates definem qual a rota escolhida

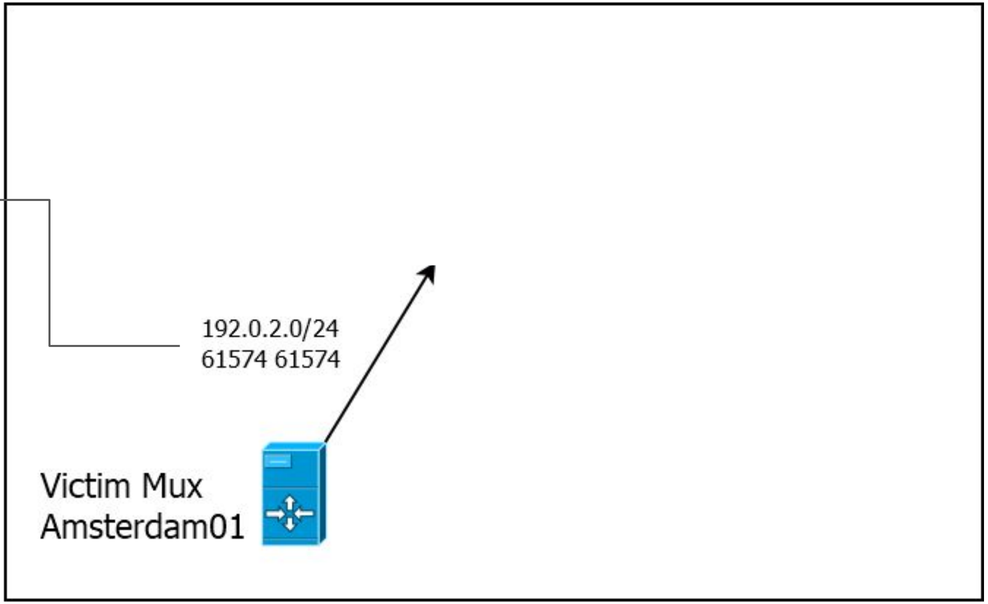
Exemplo de Configuração do Experimento

Vítima em Amsterdam



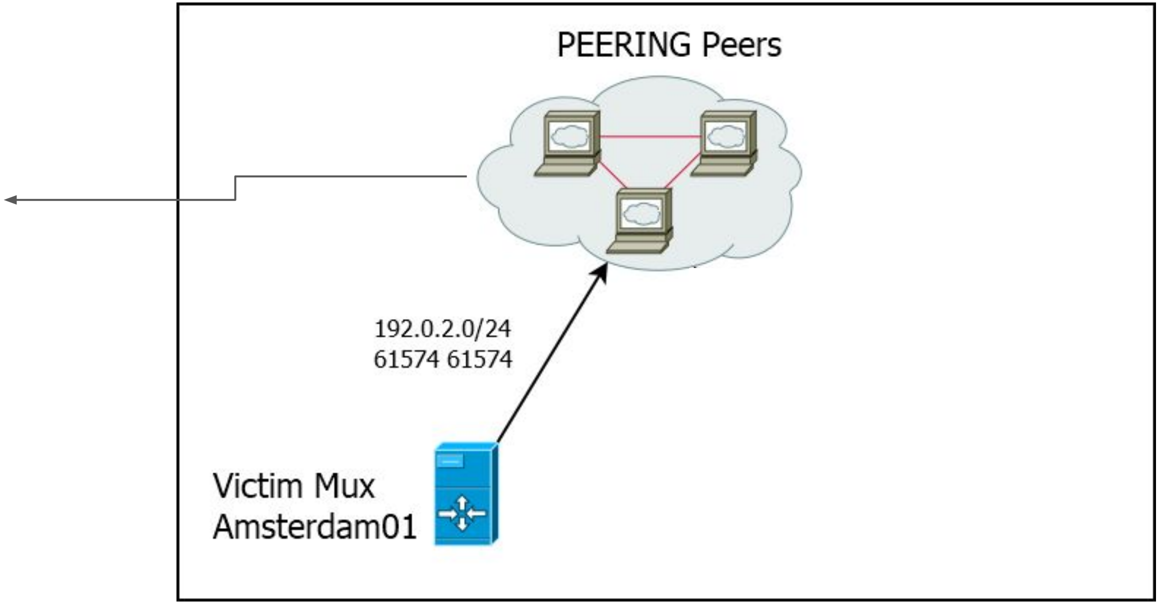
Exemplo de Configuração do Experimento

Prepend 1

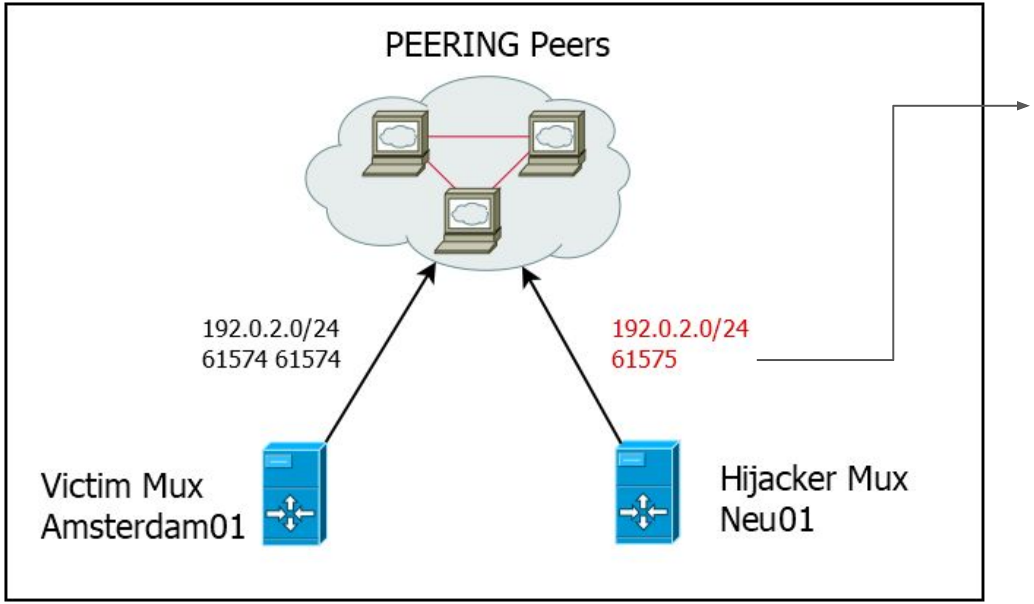


Exemplo de Configuração do Experimento

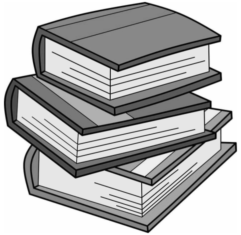
Anuncia para Peers do PEERING



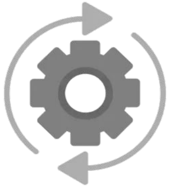
Exemplo de Configuração do Experimento



Atacante Executa um sequestro



Verificar Trabalhos Anteriores

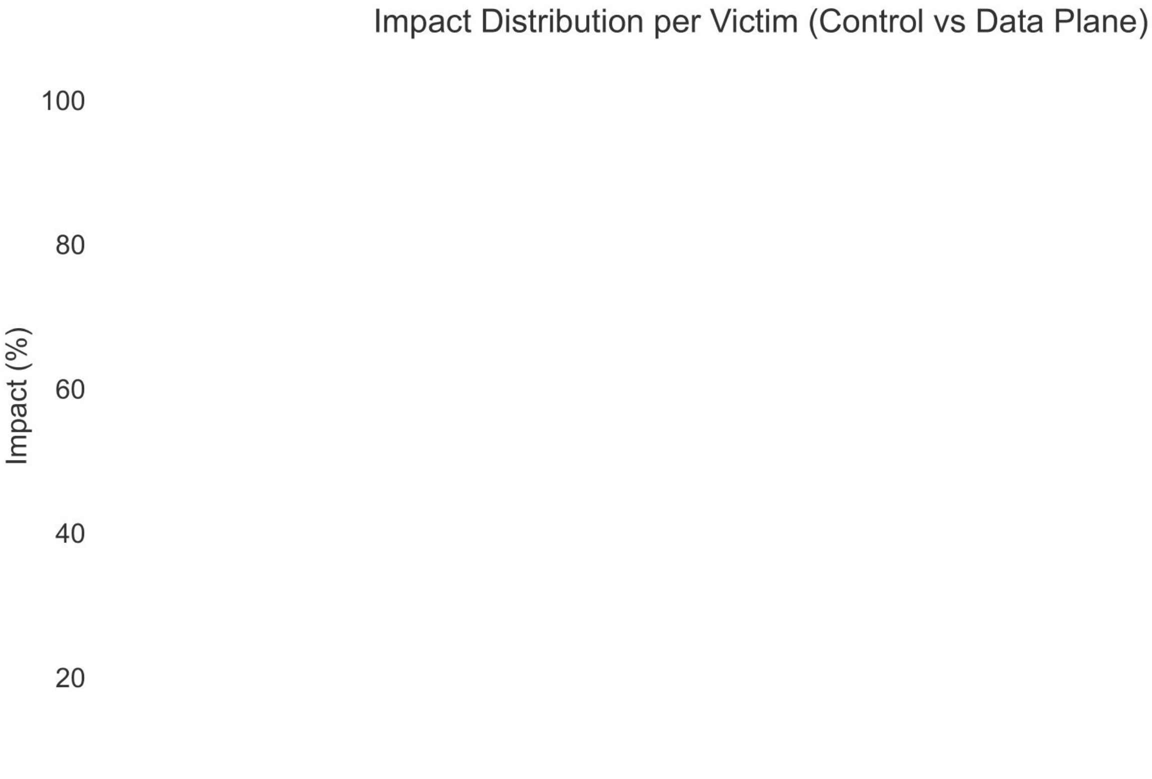


Definir uma Metodologia de Experimentos

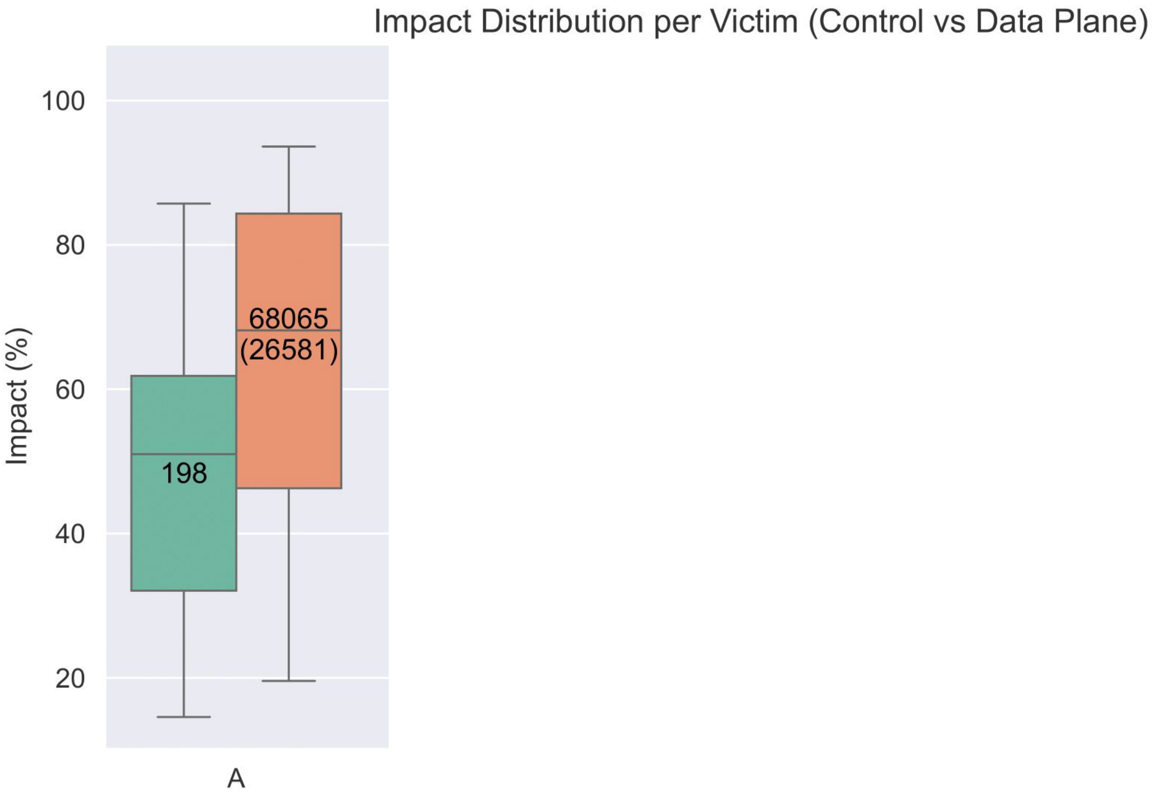
Analisar os Resultados

Definir as conclusões sobre os Resultados

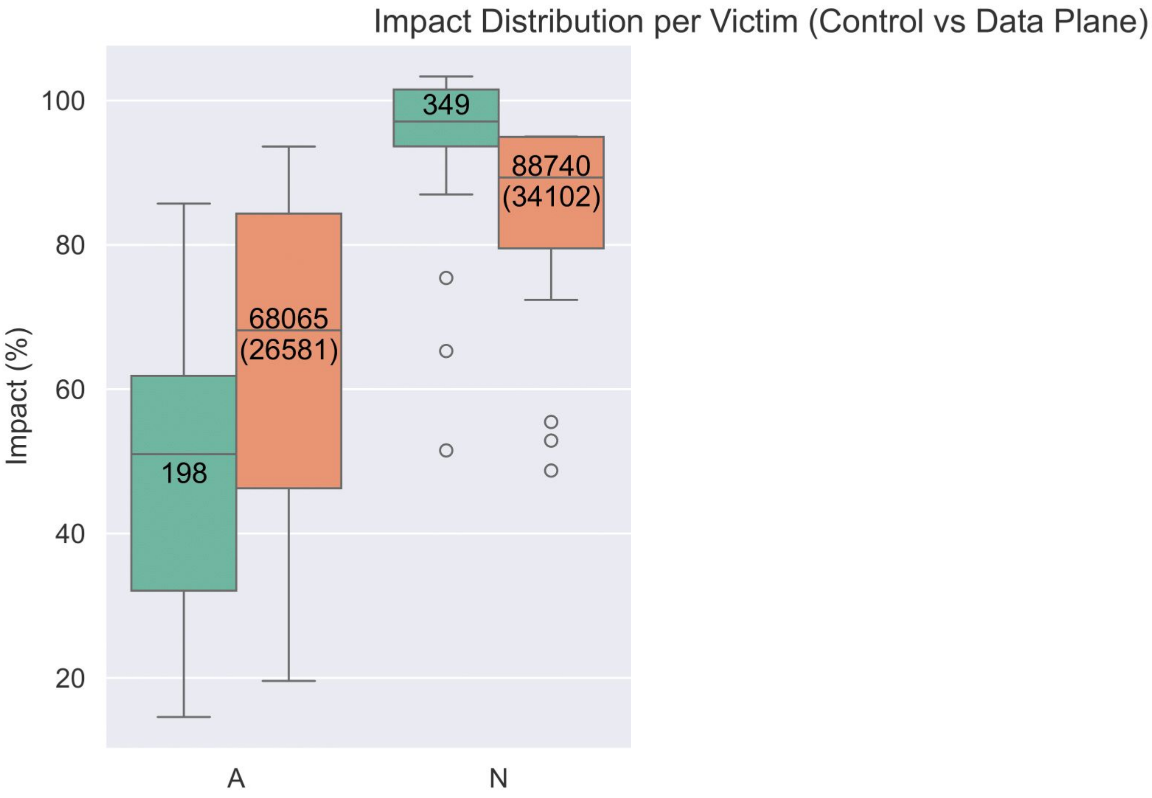
Impacto de ITE - Prepend



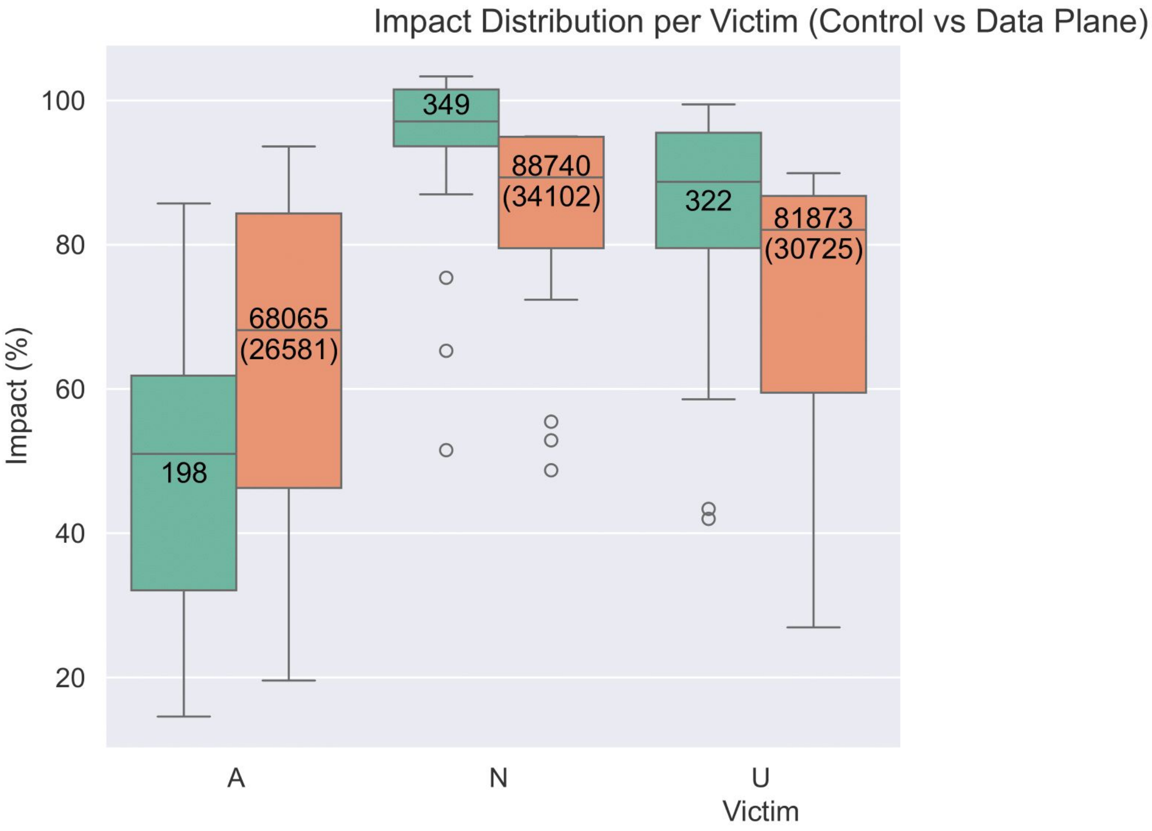
Impacto de ITE - Prepend



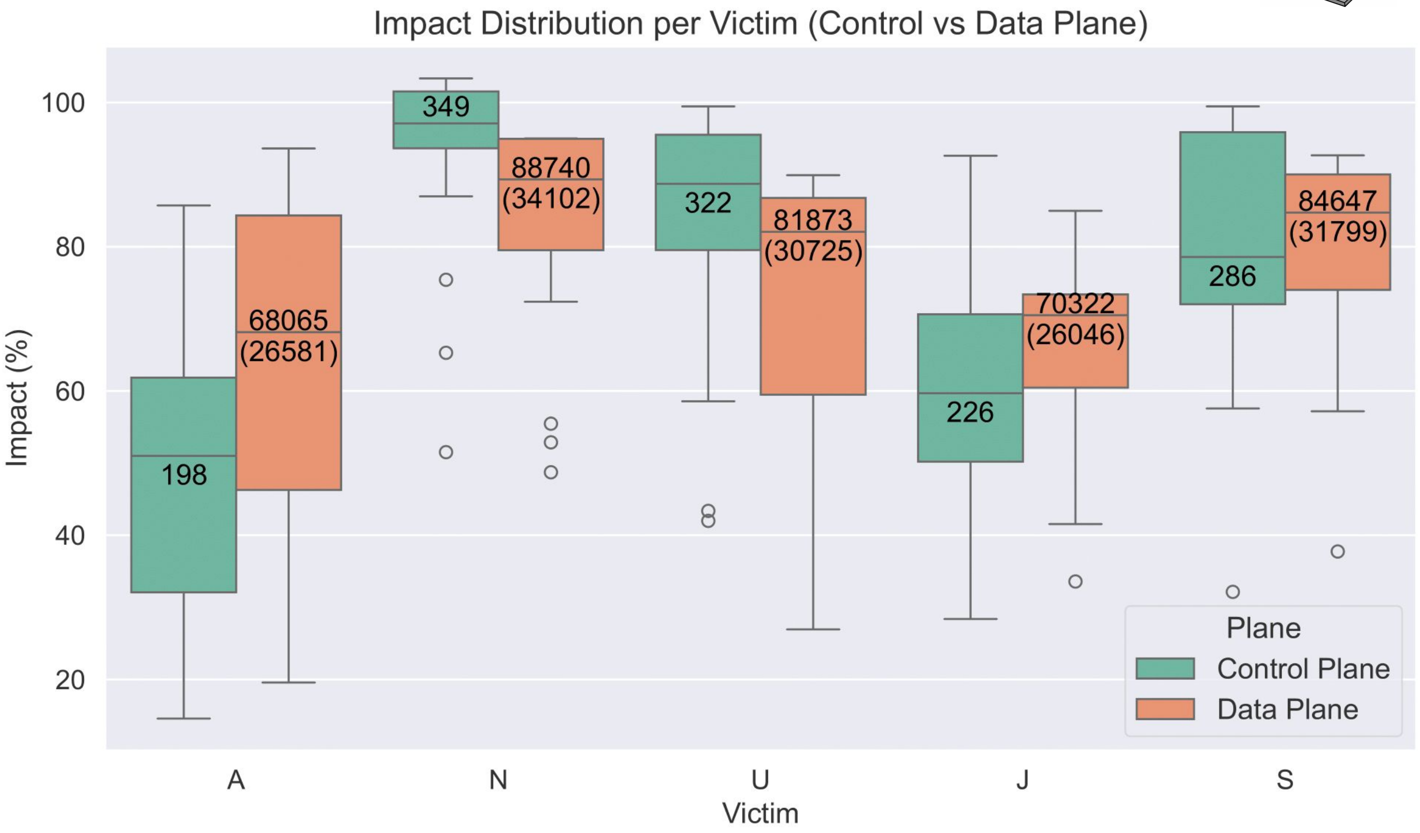
Impacto de ITE - Prepend



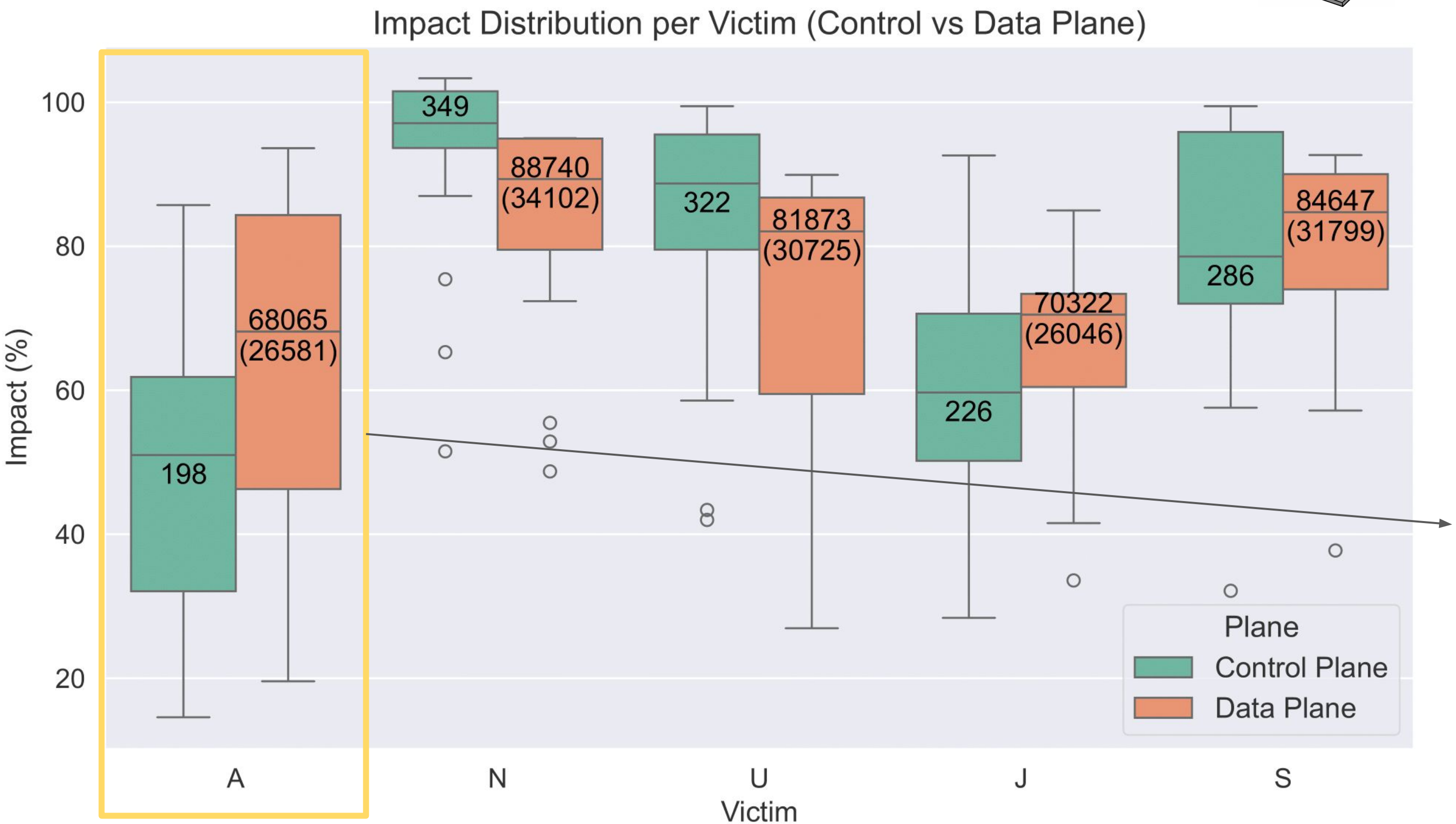
Impacto de ITE - Prepend



Impacto de ITE - Prepend

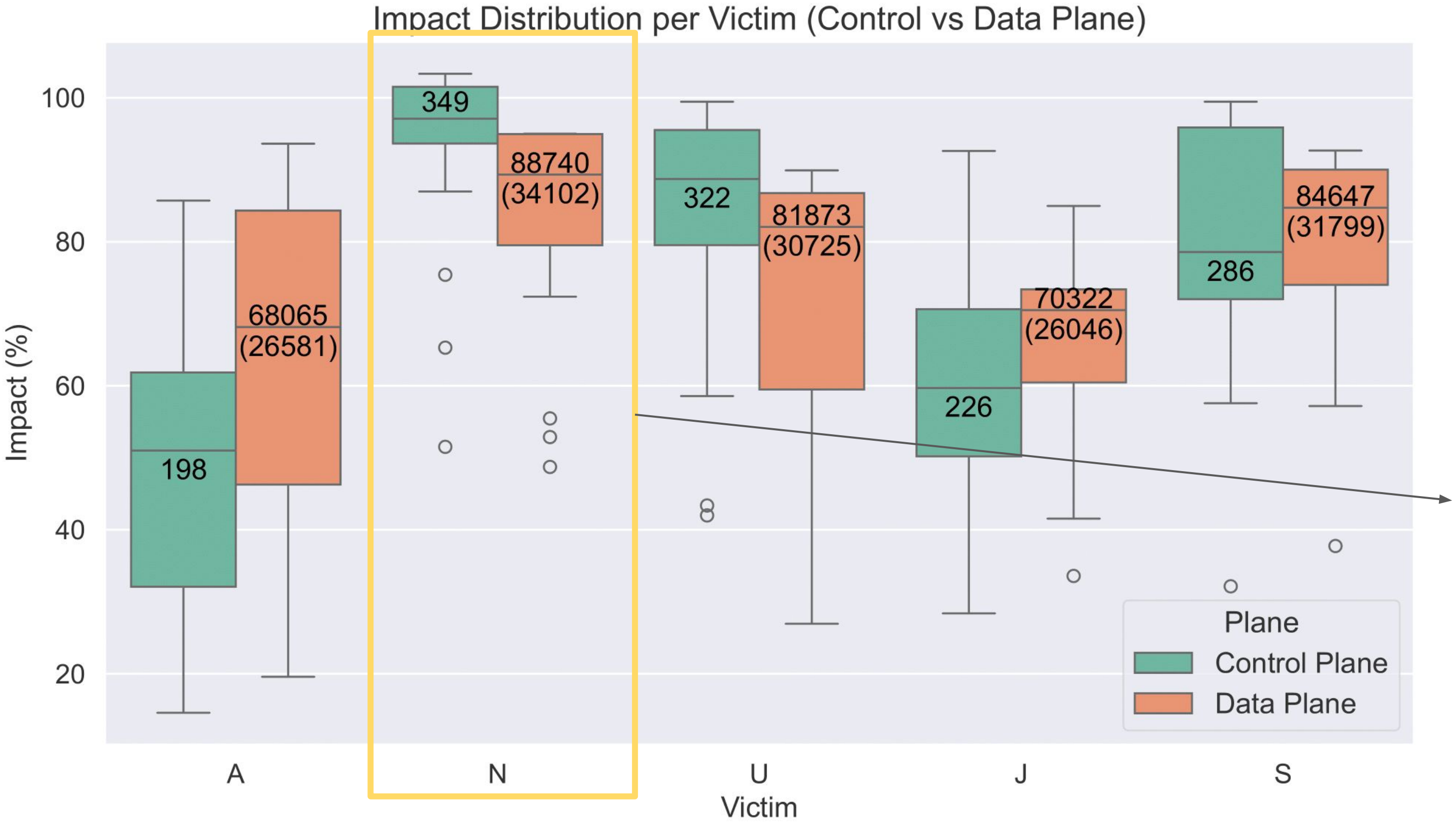


Impacto de ITE - Prepend



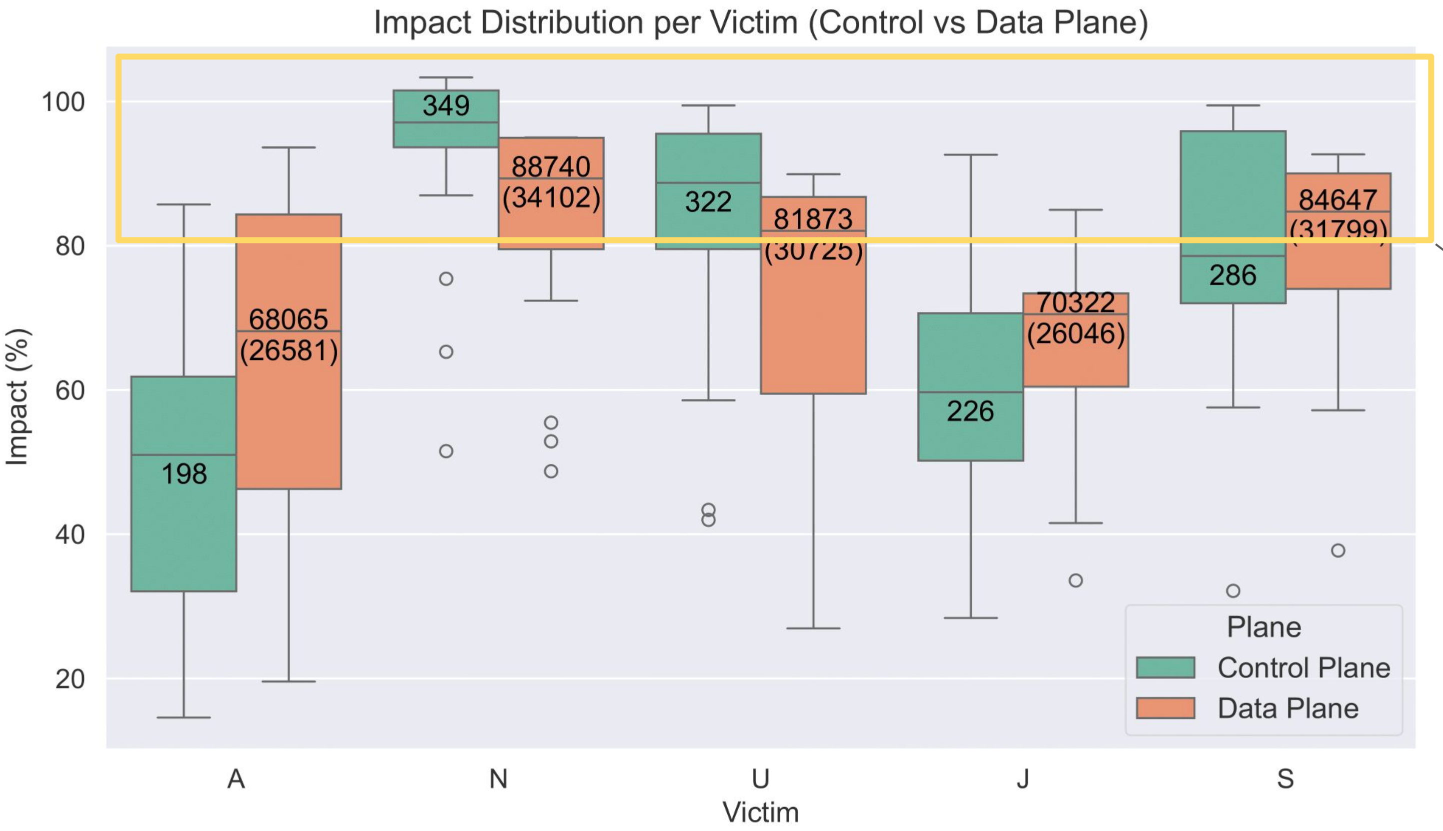
Amsterdam é pouco impactado em alguns cenários

Impacto de ITE - Prepend



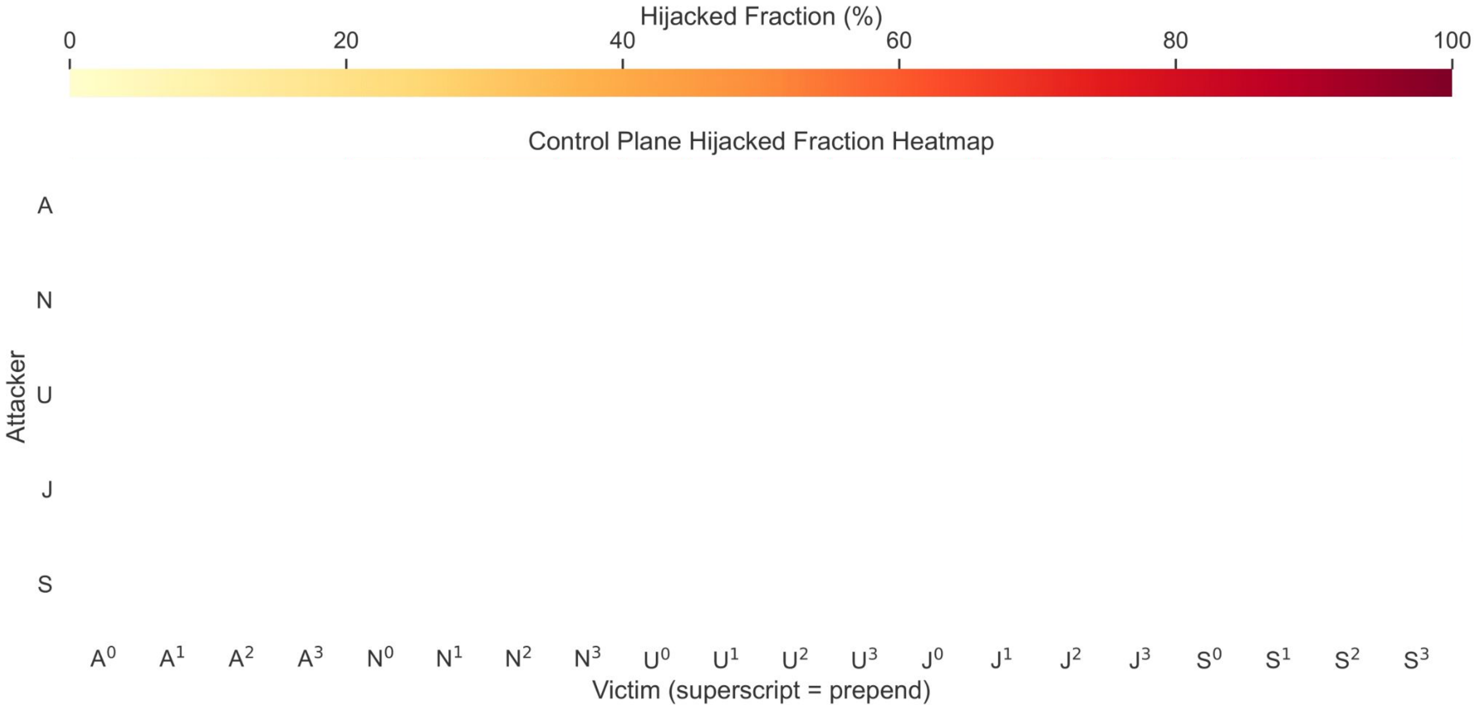
Neu01 já possui impactos mais significativos

Impacto de ITE - Prepend

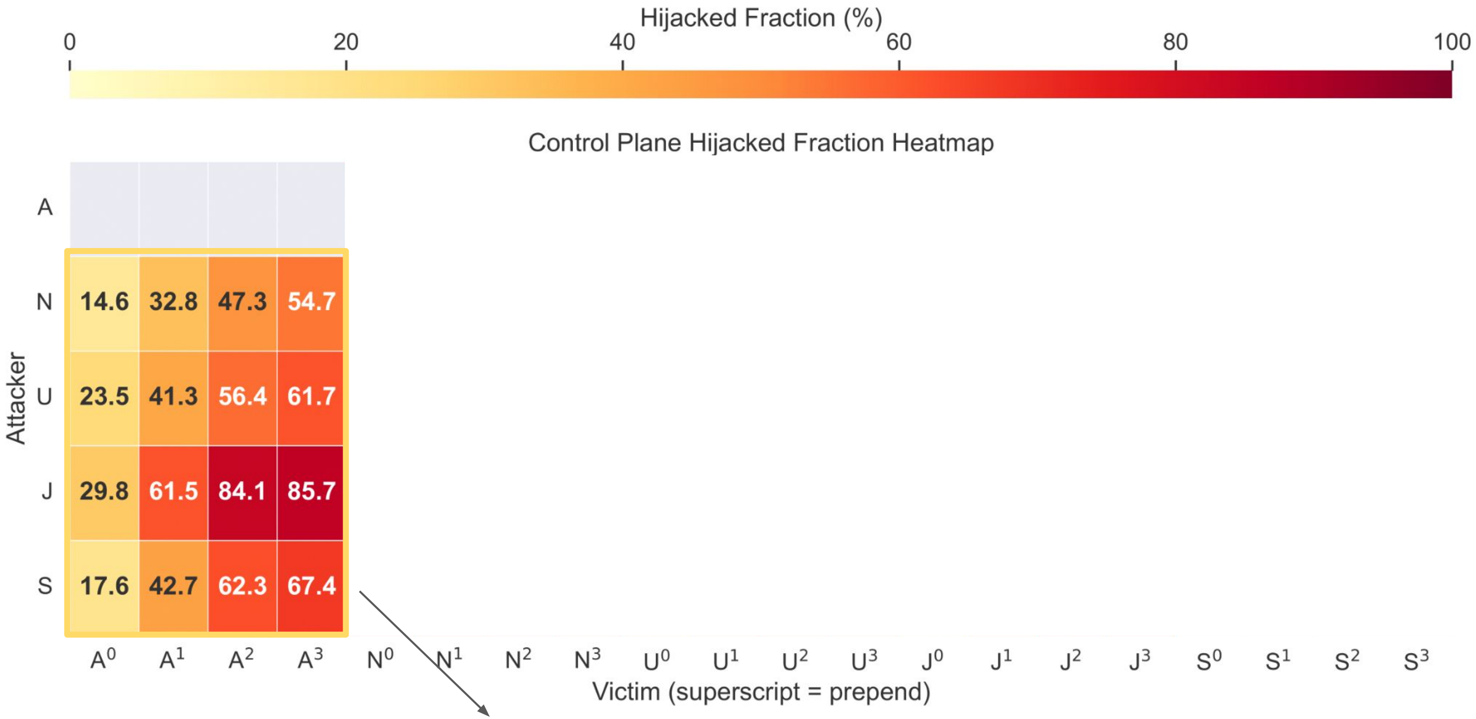


Todos muxes possuem cenários com impacto significativo

Impacto de ITE - Prepend



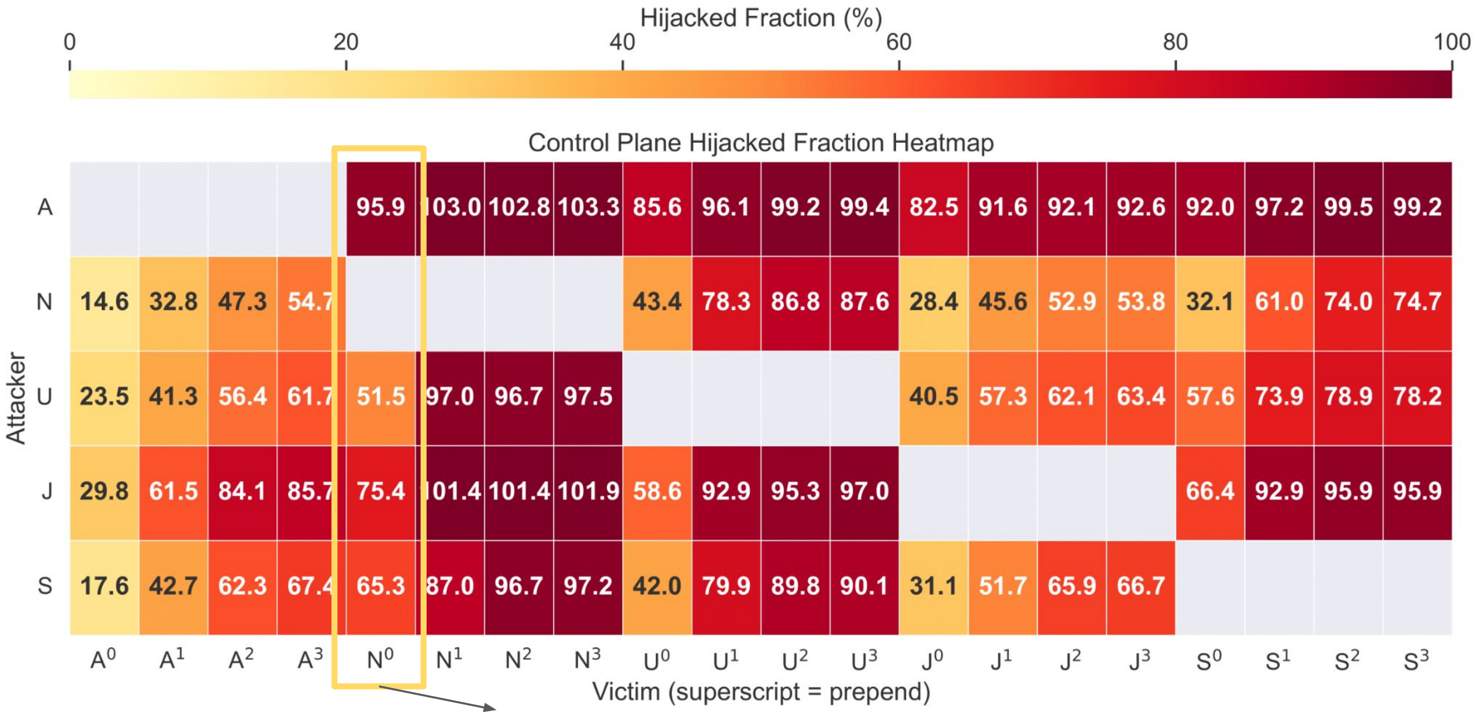
Impacto de ITE - Prepend



	A^0	A^1	A^2	A^3
A				
N	14.6	32.8	47.3	54.7
U	23.5	41.3	56.4	61.7
J	29.8	61.5	84.1	85.7
S	17.6	42.7	62.3	67.4

Aumentar o uso de prepend aumenta o impacto do sequestro

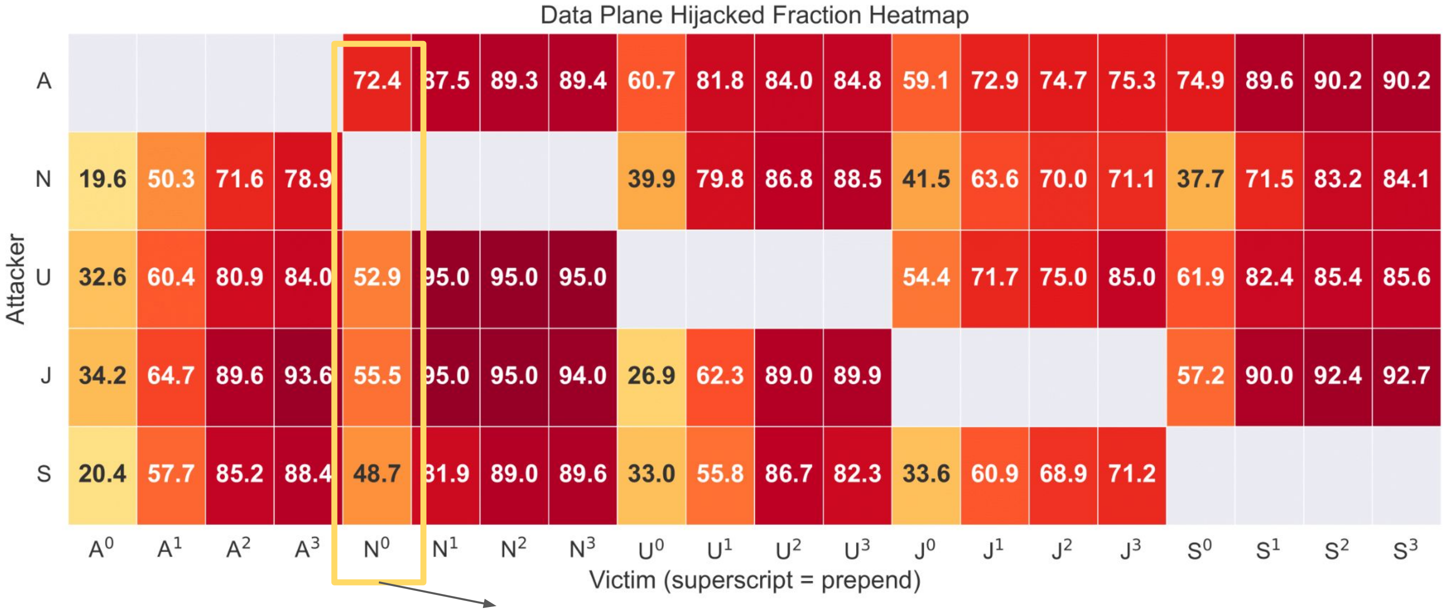
Impacto de ITE - Prepend



	A^0	A^1	A^2	A^3	N^0	N^1	N^2	N^3	U^0	U^1	U^2	U^3	J^0	J^1	J^2	J^3	S^0	S^1	S^2	S^3
A					95.9	103.0	102.8	103.3	85.6	96.1	99.2	99.4	82.5	91.6	92.1	92.6	92.0	97.2	99.5	99.2
N	14.6	32.8	47.3	54.7					43.4	78.3	86.8	87.6	28.4	45.6	52.9	53.8	32.1	61.0	74.0	74.7
U	23.5	41.3	56.4	61.7	51.5	97.0	96.7	97.5					40.5	57.3	62.1	63.4	57.6	73.9	78.9	78.2
J	29.8	61.5	84.1	85.7	75.4	101.4	101.4	101.9	58.6	92.9	95.3	97.0					66.4	92.9	95.9	95.9
S	17.6	42.7	62.3	67.4	65.3	87.0	96.7	97.2	42.0	79.9	89.8	90.1	31.1	51.7	65.9	66.7				

Entretanto ASes podem ser sofrer impactos sem nem mesmo utilizar prepends

Impacto de ITE - Prepend

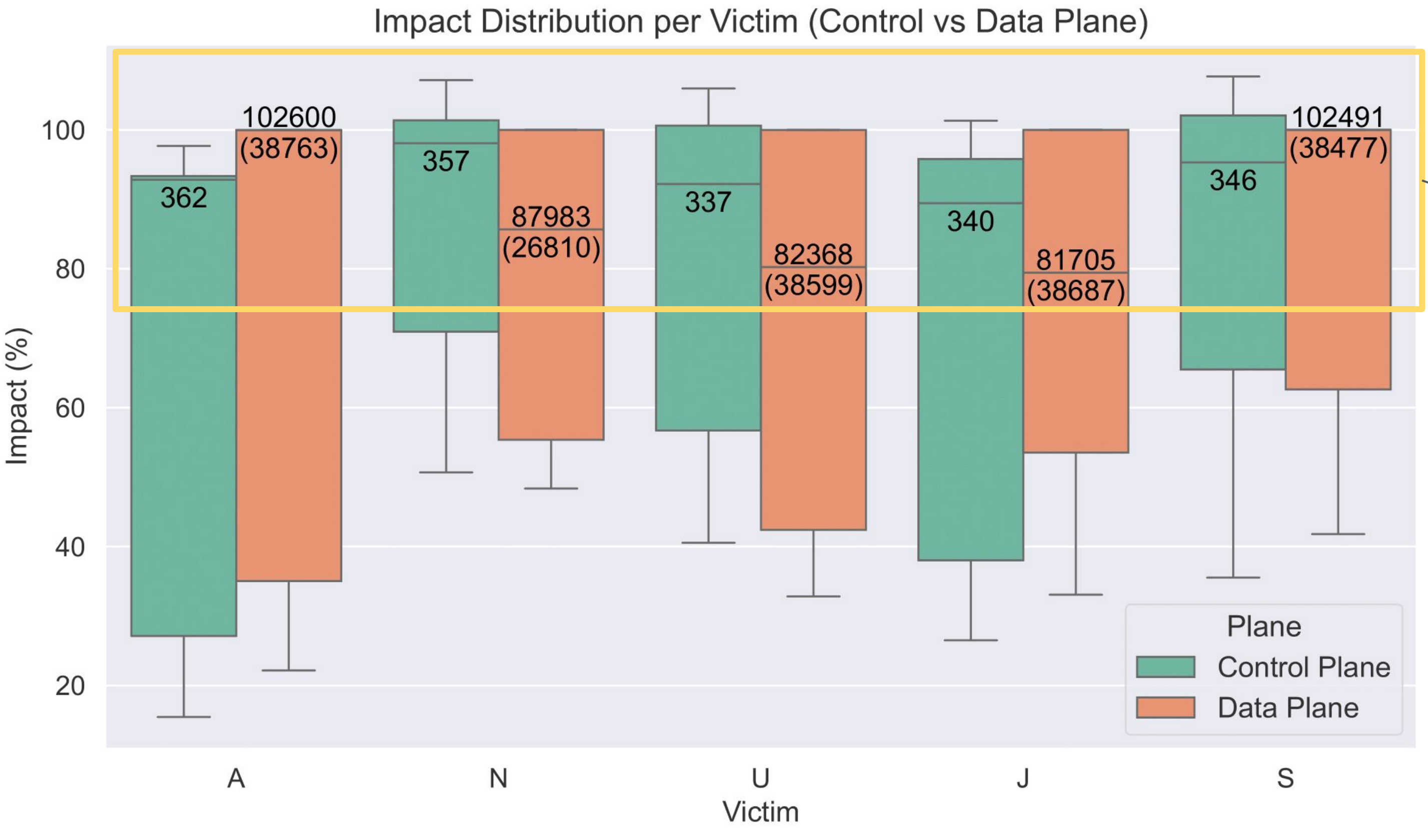


	A^0	A^1	A^2	A^3	N^0	N^1	N^2	N^3	U^0	U^1	U^2	U^3	J^0	J^1	J^2	J^3	S^0	S^1	S^2	S^3
A					72.4	87.5	89.3	89.4	60.7	81.8	84.0	84.8	59.1	72.9	74.7	75.3	74.9	89.6	90.2	90.2
N	19.6	50.3	71.6	78.9					39.9	79.8	86.8	88.5	41.5	63.6	70.0	71.1	37.7	71.5	83.2	84.1
U	32.6	60.4	80.9	84.0	52.9	95.0	95.0	95.0					54.4	71.7	75.0	85.0	61.9	82.4	85.4	85.6
J	34.2	64.7	89.6	93.6	55.5	95.0	95.0	94.0	26.9	62.3	89.0	89.9					57.2	90.0	92.4	92.7
S	20.4	57.7	85.2	88.4	48.7	81.9	89.0	89.6	33.0	55.8	86.7	82.3	33.6	60.9	68.9	71.2				

Entretanto ASes podem ser sofrer impactos sem nem mesmo utilizar prepends

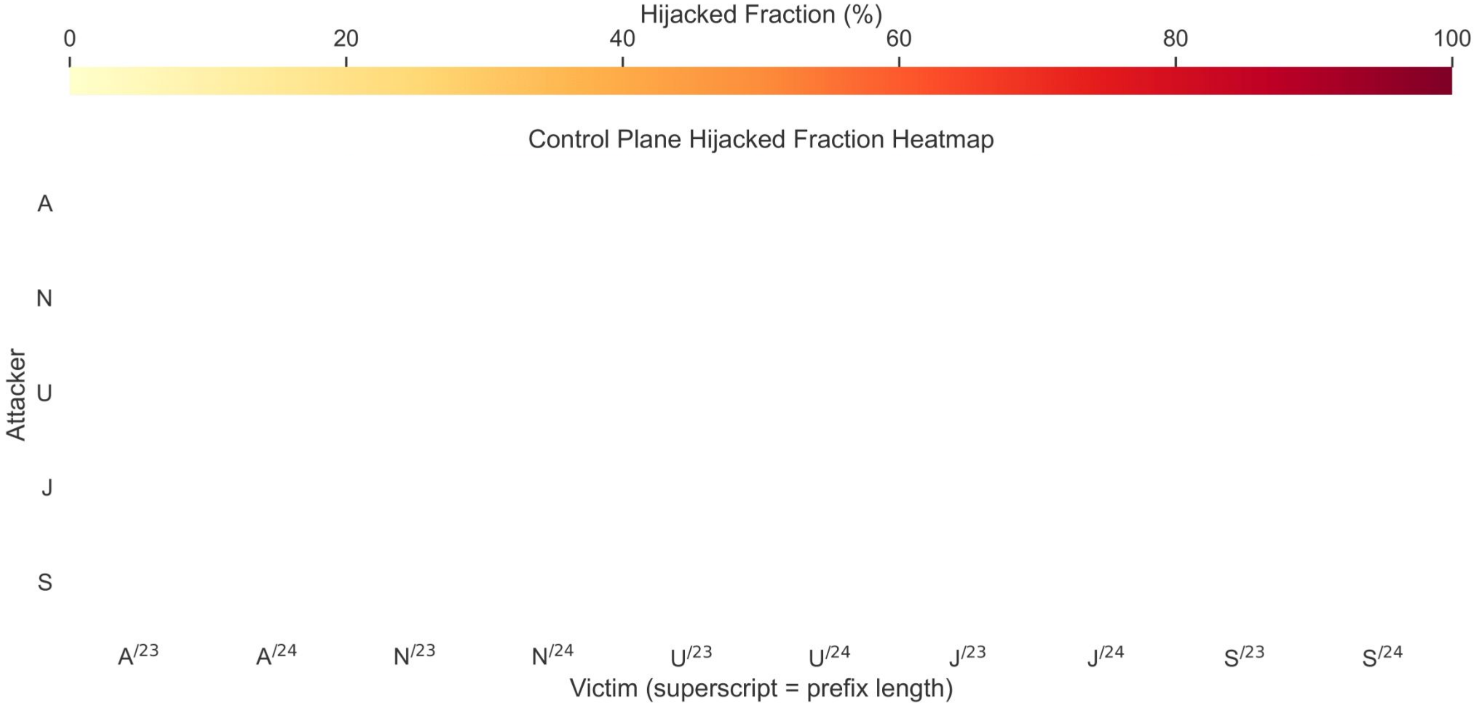
Impacto de ITE - Especificidade

Impacto de ITE - Especificidade

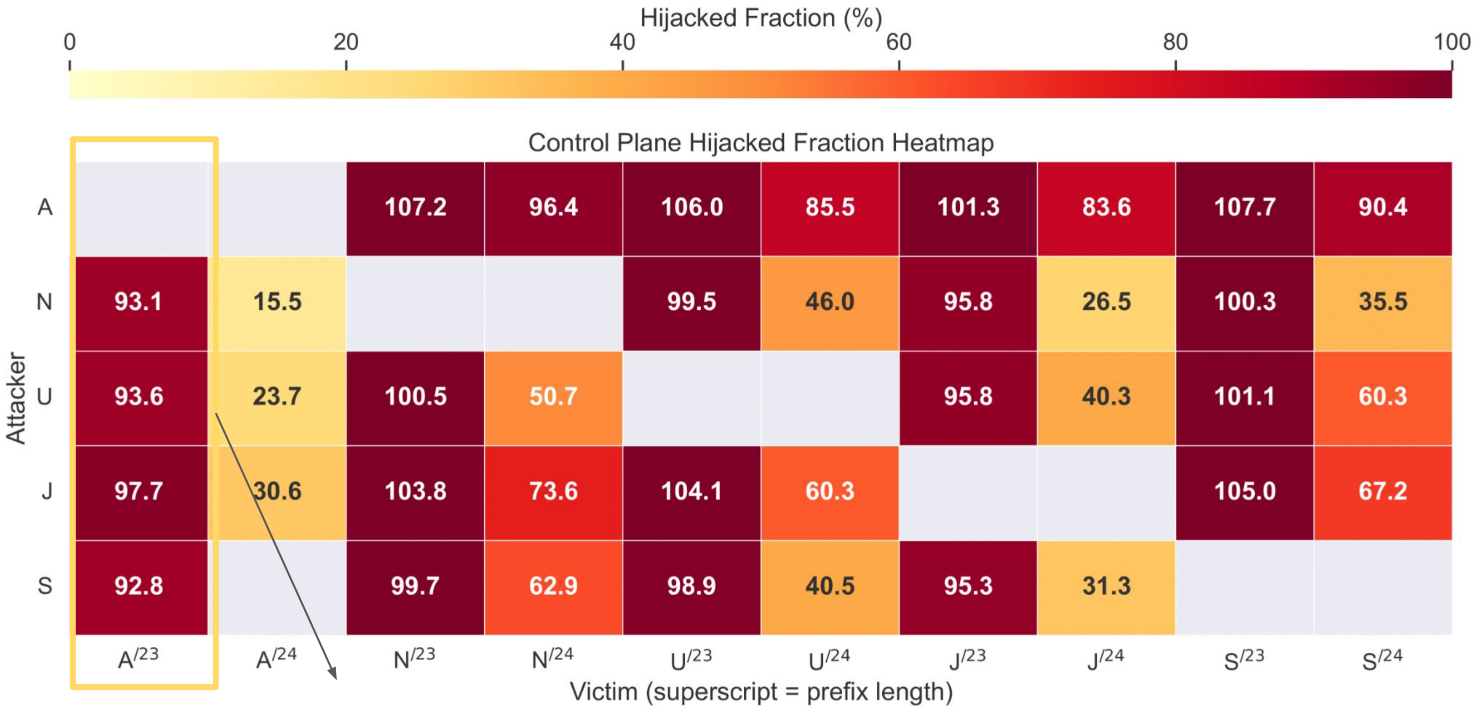


Impacto mais uniforme nos piores cenários

Impacto de ITE - Especificidade



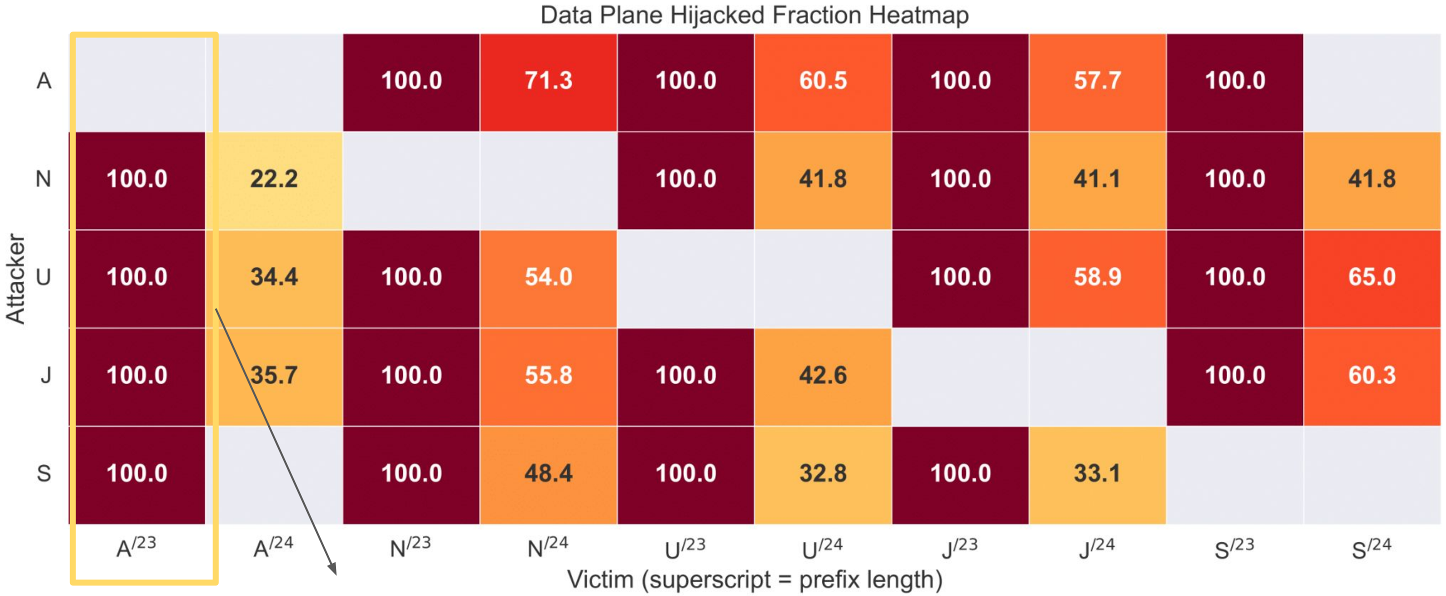
Impacto de ITE - Especificidade



Attacker	A$^{/23}$	A$^{/24}$	N$^{/23}$	N$^{/24}$	U$^{/23}$	U$^{/24}$	J$^{/23}$	J$^{/24}$	S$^{/23}$	S$^{/24}$
A			107.2	96.4	106.0	85.5	101.3	83.6	107.7	90.4
N	93.1	15.5			99.5	46.0	95.8	26.5	100.3	35.5
U	93.6	23.7	100.5	50.7			95.8	40.3	101.1	60.3
J	97.7	30.6	103.8	73.6	104.1	60.3			105.0	67.2
S	92.8		99.7	62.9	98.9	40.5	95.3	31.3		

Mesmo ASes bem conectados podem sofrer com ataques utilizando prefixos mais específicos

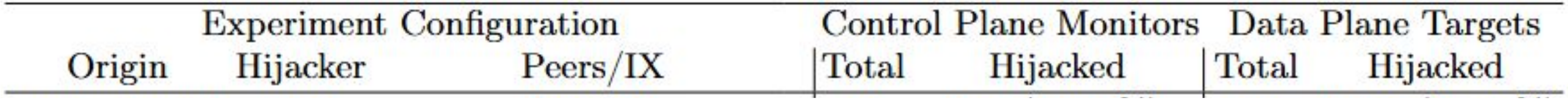
Impacto de ITE - Especificidade



Attacker	$A^{/23}$	$A^{/24}$	$N^{/23}$	$N^{/24}$	$U^{/23}$	$U^{/24}$	$J^{/23}$	$J^{/24}$	$S^{/23}$	$S^{/24}$
A			100.0	71.3	100.0	60.5	100.0	57.7	100.0	
N	100.0	22.2			100.0	41.8	100.0	41.1	100.0	41.8
U	100.0	34.4	100.0	54.0			100.0	58.9	100.0	65.0
J	100.0	35.7	100.0	55.8	100.0	42.6			100.0	60.3
S	100.0		100.0	48.4	100.0	32.8	100.0	33.1		

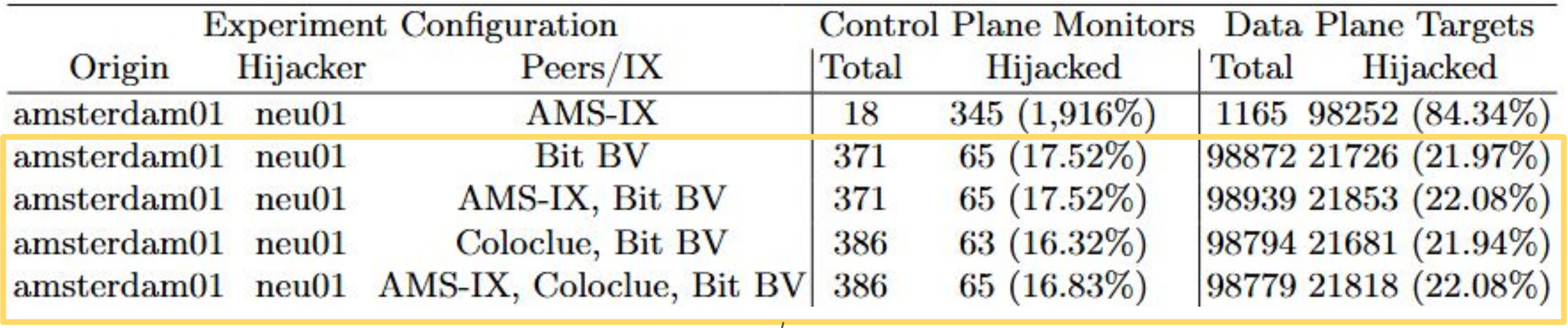
Mesmo ASes bem conectados podem sofrer com ataques utilizando prefixos mais específicos

Impacto de ITE - Seletivos



	Experiment Configuration		Control Plane Monitors		Data Plane Targets	
Origin	Hijacker	Peers/IX	Total	Hijacked	Total	Hijacked

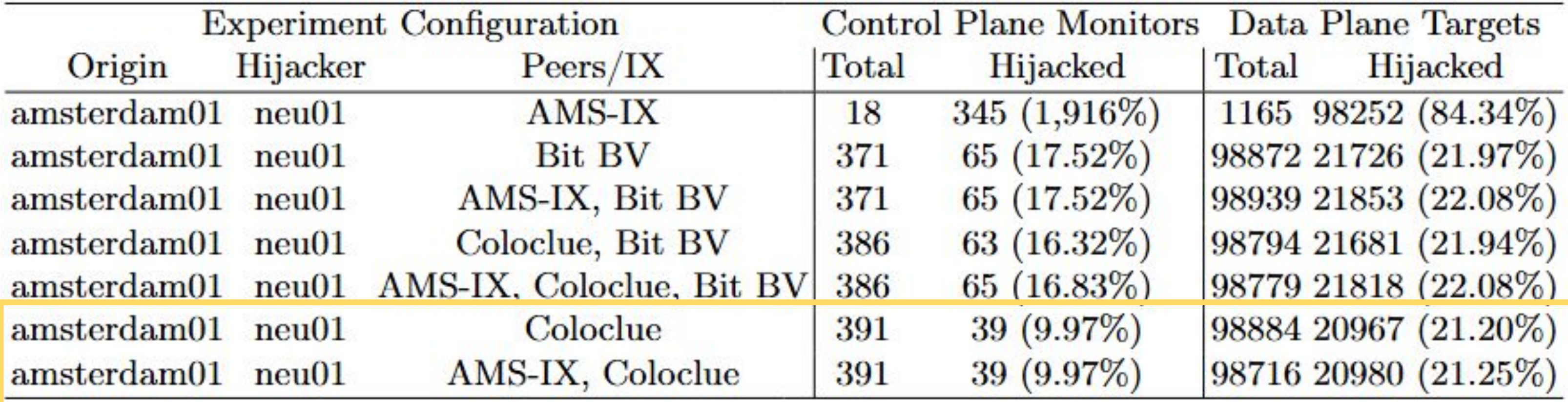
Impacto de ITE - Seletivos



Experiment Configuration			Control Plane Monitors		Data Plane Targets	
Origin	Hijacker	Peers/IX	Total	Hijacked	Total	Hijacked
amsterdam01	neu01	AMS-IX	18	345 (1,916%)	1165	98252 (84.34%)
amsterdam01	neu01	Bit BV	371	65 (17.52%)	98872	21726 (21.97%)
amsterdam01	neu01	AMS-IX, Bit BV	371	65 (17.52%)	98939	21853 (22.08%)
amsterdam01	neu01	Coloclue, Bit BV	386	63 (16.32%)	98794	21681 (21.94%)
amsterdam01	neu01	AMS-IX, Coloclue, Bit BV	386	65 (16.83%)	98779	21818 (22.08%)

Impacto similar entre diferentes configurações

Impacto de ITE - Seletivos

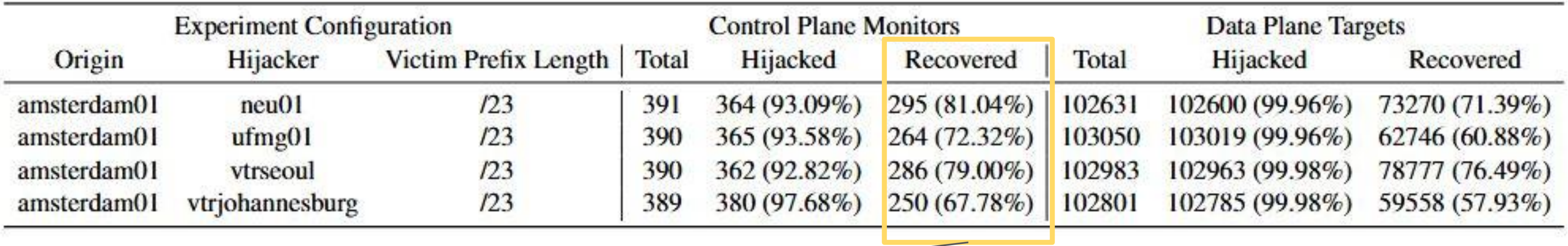


Experiment Configuration			Control Plane Monitors		Data Plane Targets	
Origin	Hijacker	Peers/IX	Total	Hijacked	Total	Hijacked
amsterdam01	neu01	AMS-IX	18	345 (1,916%)	1165	98252 (84.34%)
amsterdam01	neu01	Bit BV	371	65 (17.52%)	98872	21726 (21.97%)
amsterdam01	neu01	AMS-IX, Bit BV	371	65 (17.52%)	98939	21853 (22.08%)
amsterdam01	neu01	Coloclue, Bit BV	386	63 (16.32%)	98794	21681 (21.94%)
amsterdam01	neu01	AMS-IX, Coloclue, Bit BV	386	65 (16.83%)	98779	21818 (22.08%)
amsterdam01	neu01	Coloclue	391	39 (9.97%)	98884	20967 (21.20%)
amsterdam01	neu01	AMS-IX, Coloclue	391	39 (9.97%)	98716	20980 (21.25%)

Não anunciar para um vizinho específico leva a um impacto menor

Mitigação

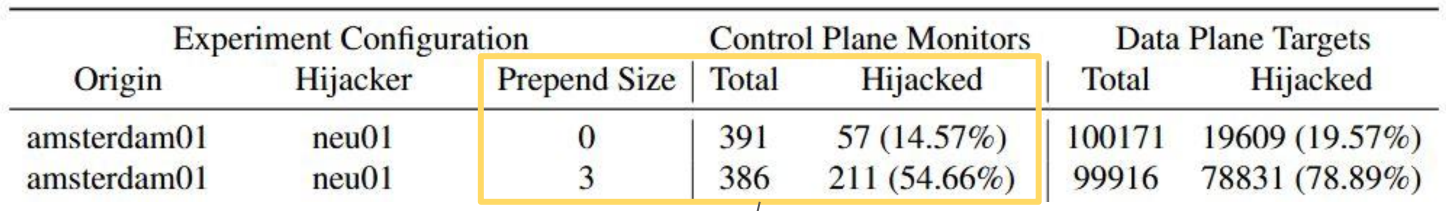
Mitigação



Experiment Configuration			Control Plane Monitors			Data Plane Targets		
Origin	Hijacker	Victim Prefix Length	Total	Hijacked	Recovered	Total	Hijacked	Recovered
amsterdam01	neu01	/23	391	364 (93.09%)	295 (81.04%)	102631	102600 (99.96%)	73270 (71.39%)
amsterdam01	ufmg01	/23	390	365 (93.58%)	264 (72.32%)	103050	103019 (99.96%)	62746 (60.88%)
amsterdam01	vtrseoul	/23	390	362 (92.82%)	286 (79.00%)	102983	102963 (99.98%)	78777 (76.49%)
amsterdam01	vtrjohannesburg	/23	389	380 (97.68%)	250 (67.78%)	102801	102785 (99.98%)	59558 (57.93%)

Ao Mitigar um sequestro (feito com um /24) utilizando um prefixo /24, a recuperação fica então ligada a preferência local e tamanho de caminhos

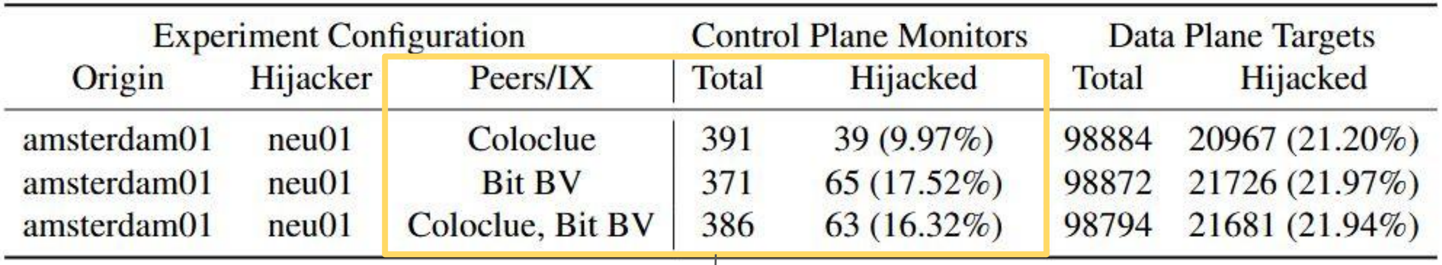
Mitigação



Experiment Configuration			Control Plane Monitors		Data Plane Targets	
Origin	Hijacker	Prepend Size	Total	Hijacked	Total	Hijacked
amsterdam01	neu01	0	391	57 (14.57%)	100171	19609 (19.57%)
amsterdam01	neu01	3	386	211 (54.66%)	99916	78831 (78.89%)

Remover prepends ajuda no quesito de tamanho de caminhos.

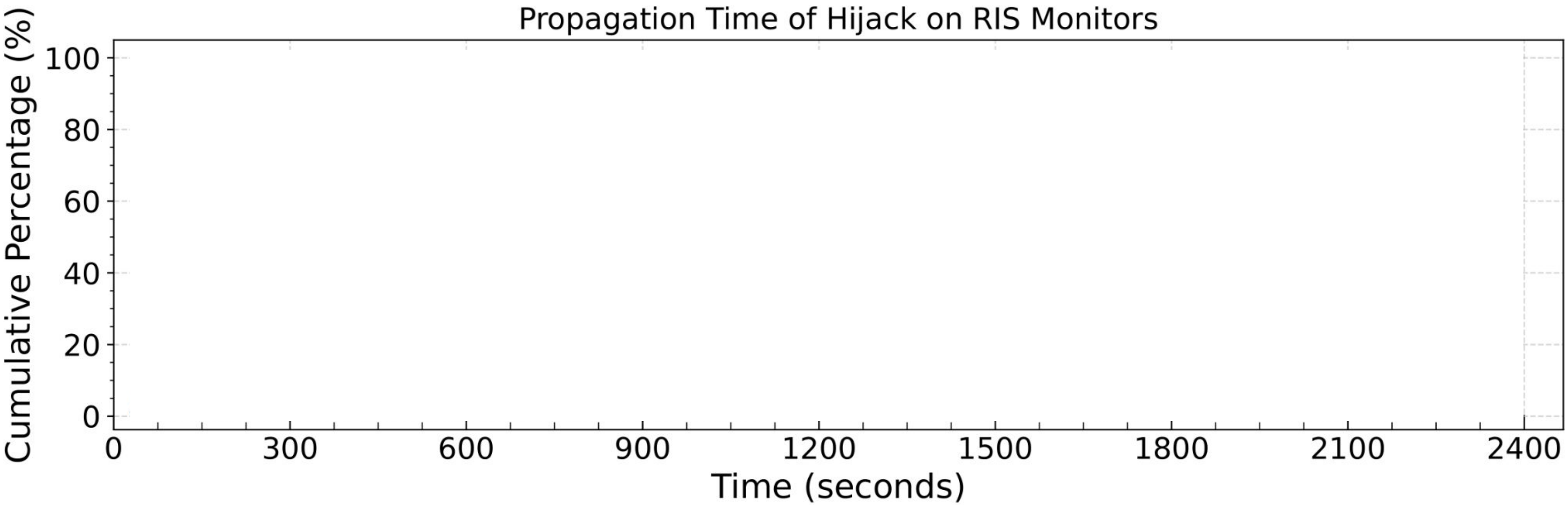
Mitigação



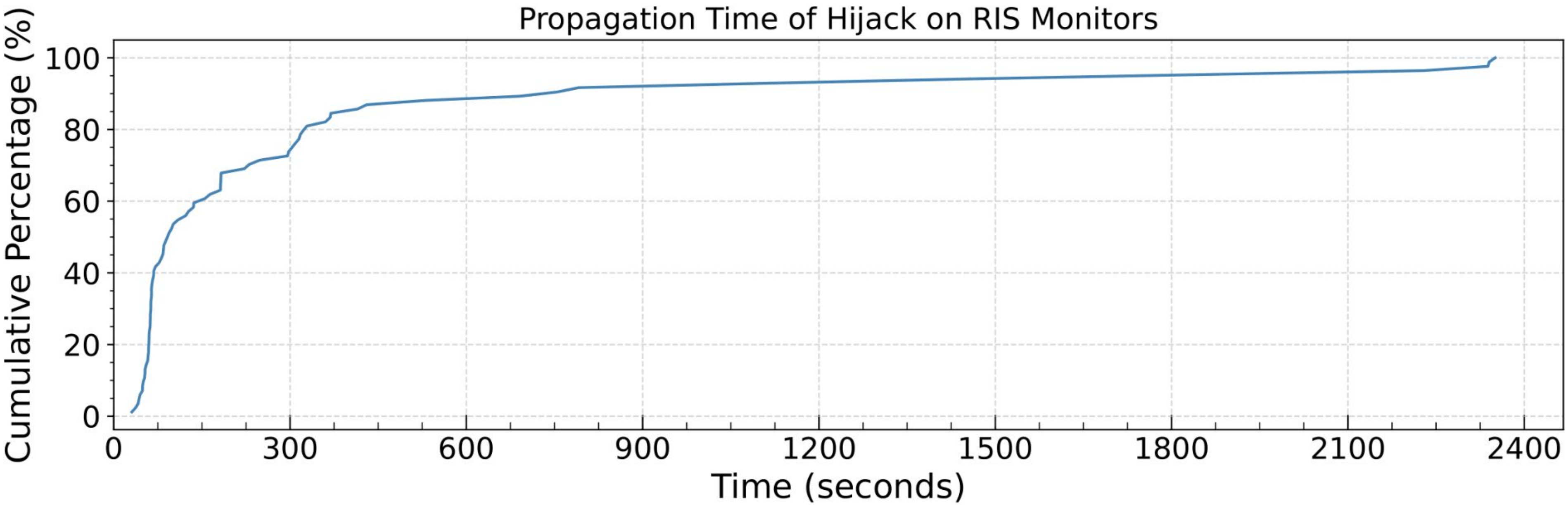
Experiment Configuration			Control Plane Monitors		Data Plane Targets	
Origin	Hijacker	Peers/IX	Total	Hijacked	Total	Hijacked
amsterdam01	neu01	Coloclue	391	39 (9.97%)	98884	20967 (21.20%)
amsterdam01	neu01	Bit BV	371	65 (17.52%)	98872	21726 (21.97%)
amsterdam01	neu01	Coloclue, Bit BV	386	63 (16.32%)	98794	21681 (21.94%)

Ajustar anúncios seletivos também pode diminuir o impacto

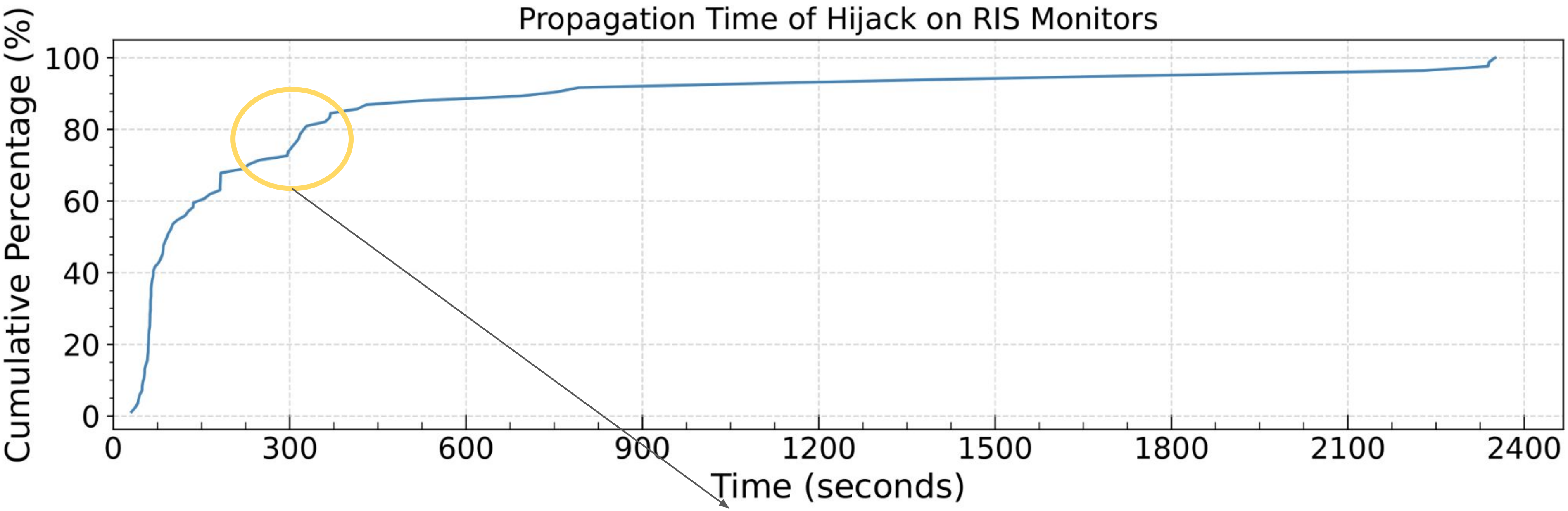
ASes Impactados



ASes Impactados

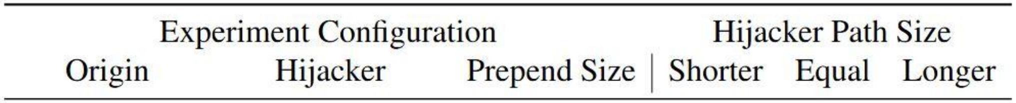


ASes Impactados



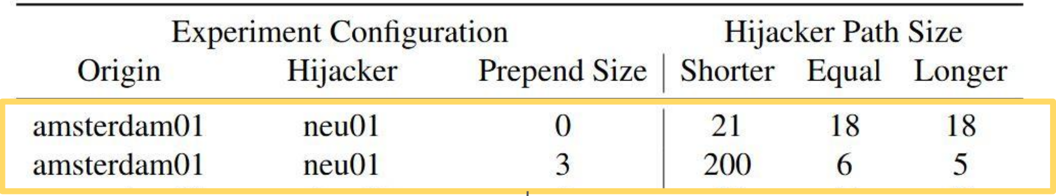
Em 5 minutos, para 74% dos experimentos o sequestro já havia atingido o ápice em monitores do RIS

ASes Impactados



Experiment Configuration			Hijacker Path Size		
Origin	Hijacker	Prepend Size	Shorter	Equal	Longer

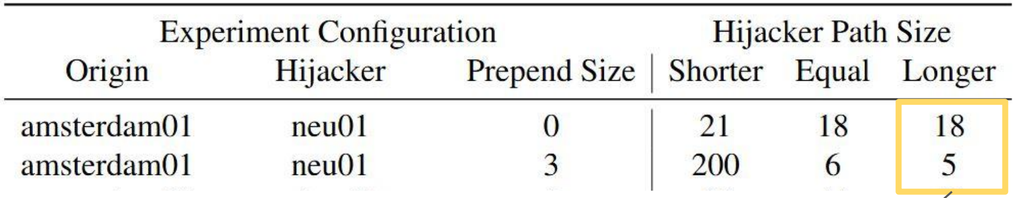
ASes Impactados



Experiment Configuration			Hijacker Path Size		
Origin	Hijacker	Prepend Size	Shorter	Equal	Longer
amsterdam01	neu01	0	21	18	18
amsterdam01	neu01	3	200	6	5

Ao utilizar prepends mais longos, os sequestros acontecem, em maioria, pelo sequestrados possuir um caminho mais curto

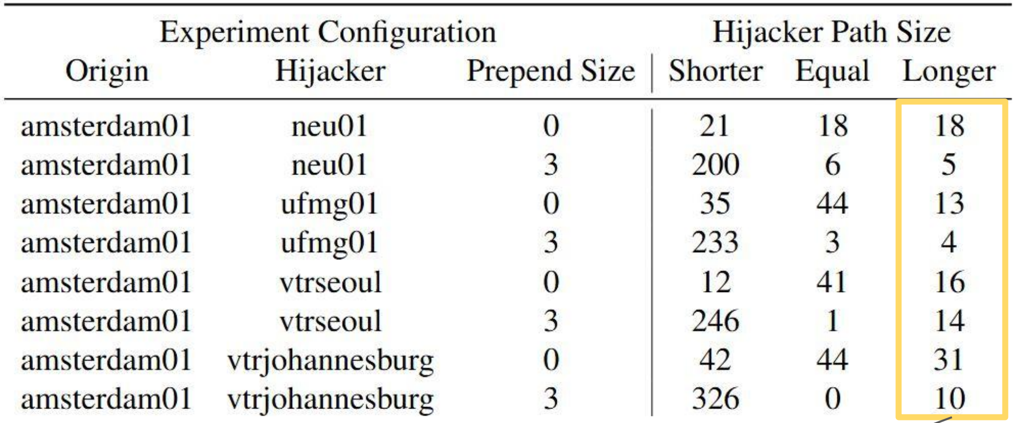
ASes Impactados



Experiment Configuration			Hijacker Path Size		
Origin	Hijacker	Prepend Size	Shorter	Equal	Longer
amsterdam01	neu01	0	21	18	18
amsterdam01	neu01	3	200	6	5

Entretanto há casos em que monitores foram sequestrados devido a preferência local em algum momento do AS-path

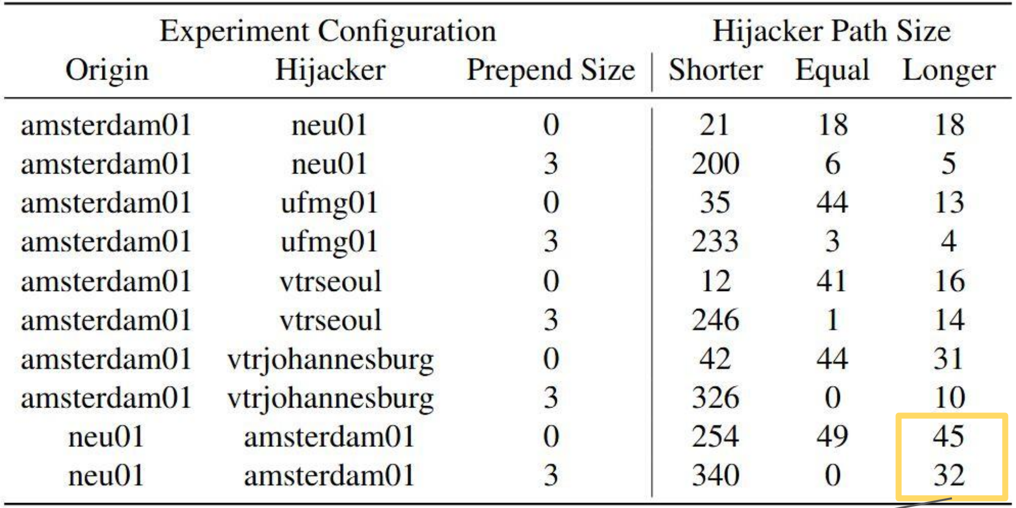
ASes Impactados



Experiment Configuration			Hijacker Path Size		
Origin	Hijacker	Prepend Size	Shorter	Equal	Longer
amsterdam01	neu01	0	21	18	18
amsterdam01	neu01	3	200	6	5
amsterdam01	ufmg01	0	35	44	13
amsterdam01	ufmg01	3	233	3	4
amsterdam01	vtrseoul	0	12	41	16
amsterdam01	vtrseoul	3	246	1	14
amsterdam01	vtrjohannesburg	0	42	44	31
amsterdam01	vtrjohannesburg	3	326	0	10

Entretanto há casos em que monitores foram sequestrados devido a preferência local em algum momento do AS-path

ASes Impactados



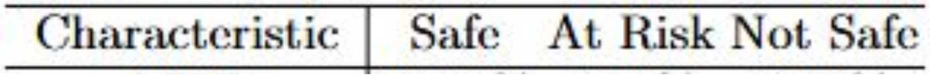
Experiment Configuration			Hijacker Path Size		
Origin	Hijacker	Prepend Size	Shorter	Equal	Longer
amsterdam01	neu01	0	21	18	18
amsterdam01	neu01	3	200	6	5
amsterdam01	ufmg01	0	35	44	13
amsterdam01	ufmg01	3	233	3	4
amsterdam01	vtrseoul	0	12	41	16
amsterdam01	vtrseoul	3	246	1	14
amsterdam01	vtrjohannesburg	0	42	44	31
amsterdam01	vtrjohannesburg	3	326	0	10
neu01	amsterdam01	0	254	49	45
neu01	amsterdam01	3	340	0	32

Quando amsterdam01 sequestra neu01 45 monitores já escolhem por preferência local

Cenário Atual

Cenário Atual

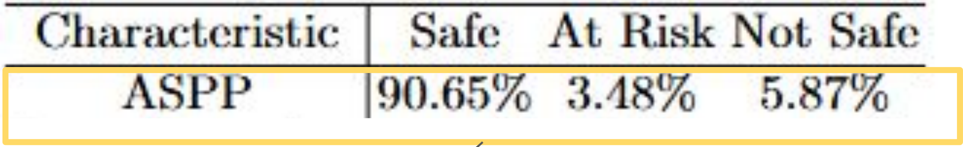
- Uso de Prepend
  - 0-1: Seguro
  - 2: Em Risco
  - 3 ou Mais: Inseguro



Characteristic	Safe	At Risk	Not Safe

Cenário Atual

- Uso de Prepend
  - 0-1: Seguro
  - 2: Em Risco
  - 3 ou Mais: Inseguro



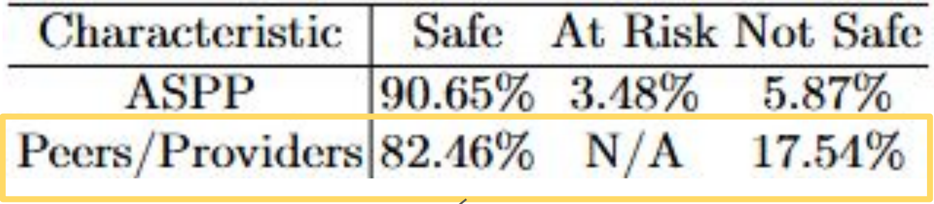
Characteristic	Safe	At Risk	Not Safe
ASPP	90.65%	3.48%	5.87%

Maioria do espaço de endereçamento não utiliza prepends ou utiliza com tamanho 1

Cenário Atual

- Uso de Prepend
  - 0-1: Seguro
  - 2: Em Risco
  - 3 ou Mais: Inseguro

- Peers/Providers
  - 1: Inseguro
  - 2 ou Mais: Seguro



Characteristic	Safe	At Risk	Not Safe
ASPP	90.65%	3.48%	5.87%
Peers/Providers	82.46%	N/A	17.54%

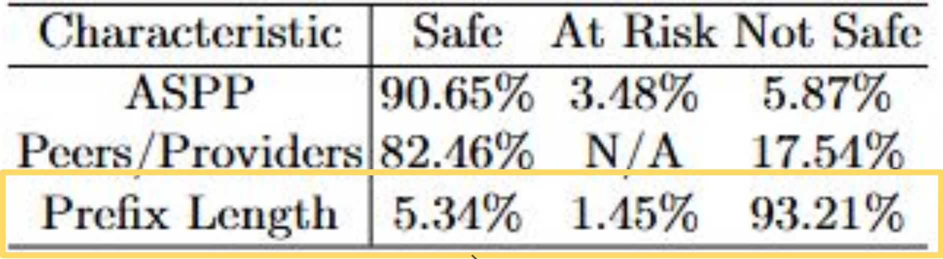
Maioria do espaço de endereçamento está anunciado em ASes com pelo menos 2 Peers/Providers

Cenário Atual

- Uso de Prepend
  - 0-1: Seguro
  - 2: Em Risco
  - 3 ou Mais: Inseguro

- Peers/Providers
  - 1: Inseguro
  - 2 ou Mais: Seguro

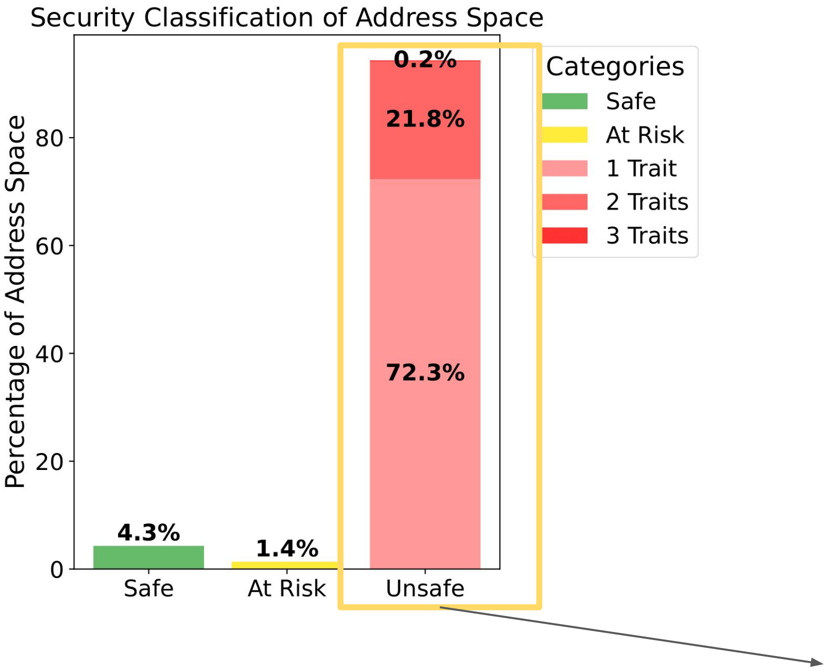
- Especificidade
  - /24: Seguro
  - /23: Em Risco
  - /22 ou Menos Específico: Inseguro



Characteristic	Safe	At Risk	Not Safe
ASPP	90.65%	3.48%	5.87%
Peers/Providers	82.46%	N/A	17.54%
Prefix Length	5.34%	1.45%	93.21%

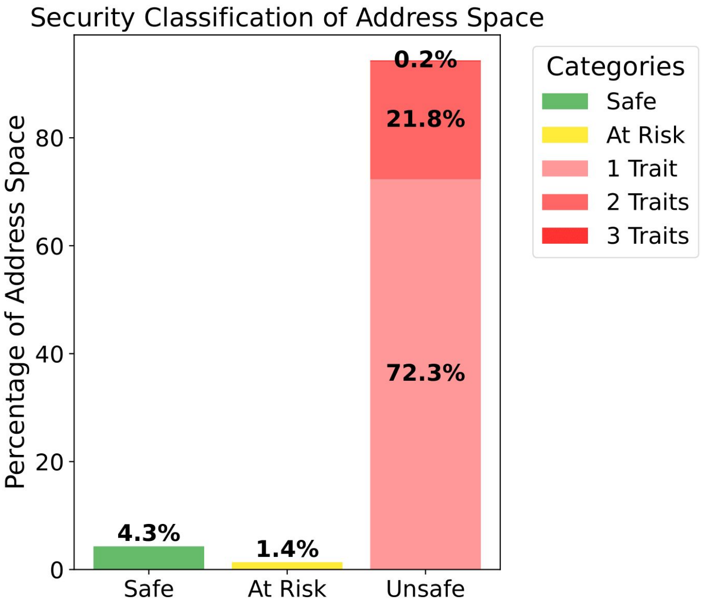
Maioria do espaço está em anúncios menos específicos que /23

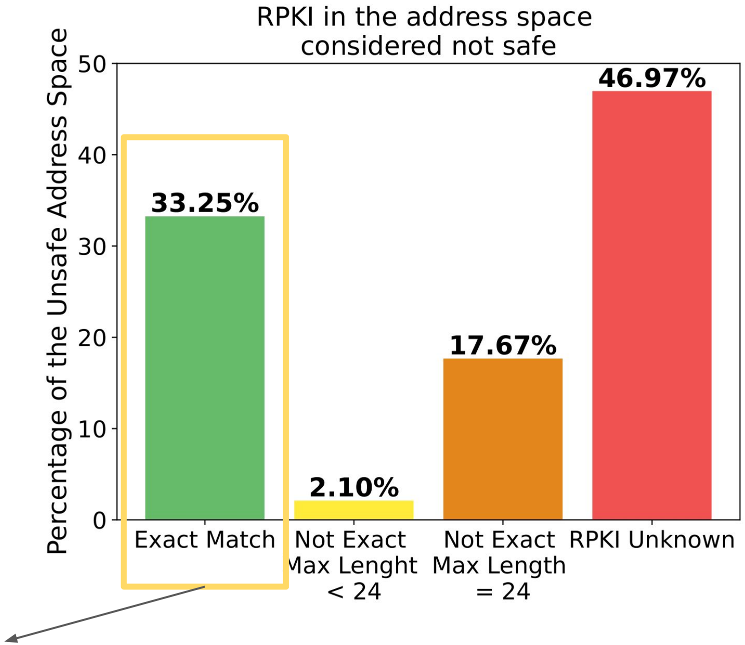
Cenário Atual



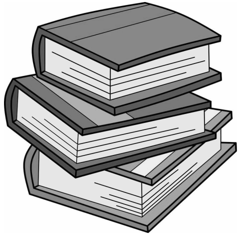
Ao combinar as três análises, a maioria do espaço possui características que podem facilitar o impacto de um sequestro de prefixo

Cenário Atual

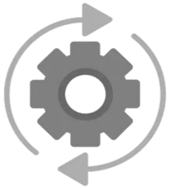




Do espaço que consideramos inseguro, apenas 33.25% do espaço de endereçamento tem ROAs com max length igual ao anúncio.



Verificar Trabalhos Anteriores



Definir uma Metodologia de Experimentos

Analisar os Resultados

Definir as conclusões sobre os Resultados

Em Resumo…

Ainda existem desafios de roteamento, logo ITE são usadas

Em Resumo…

Ainda existem desafios de roteamento, logo ITE são usadas

PEERING para realizar os experimentos

Em Resumo…

Ainda existem desafios de roteamento, logo ITE são usadas

PEERING para realizar os experimentos

RQ1:As técnicas influenciam a chance de um sequestro, ataques com prefixos mais específico são eficientes.

Em Resumo…

Ainda existem desafios de roteamento, logo ITE são usadas

PEERING para realizar os experimentos

RQ1:As técnicas influenciam a chance de um sequestro, ataques com prefixos mais específico são eficientes.

RQ2-3: ASes melhor conectados impactam mais. Qualidade das conexões pode ser mais importante que quantidade

Em Resumo…

Ainda existem desafios de roteamento, logo ITE são usadas

PEERING para realizar os experimentos

RQ1:As técnicas influenciam a chance de um sequestro, ataques com prefixos mais específico são eficientes.

RQ2-3: ASes melhor conectados impactam mais. Qualidade das conexões pode ser mais importante que quantidade

RQ4: Caminhos menores são grande parte dos impactos. Preferência local influencia.

Em Resumo…

Ainda existem desafios de roteamento, logo ITE são usadas

PEERING para realizar os experimentos

RQ1:As técnicas influenciam a chance de um sequestro, ataques com prefixos mais específico são eficientes.

RQ2-3: ASes melhor conectados impactam mais. Qualidade das conexões pode ser mais importante que quantidade

RQ4: Caminhos menores são grande parte dos impactos. Preferência local influencia.

RQ5: 61.4% do espaço de endereçamento possui riscos.

Renan Barreto
renan.barreto@furg.br