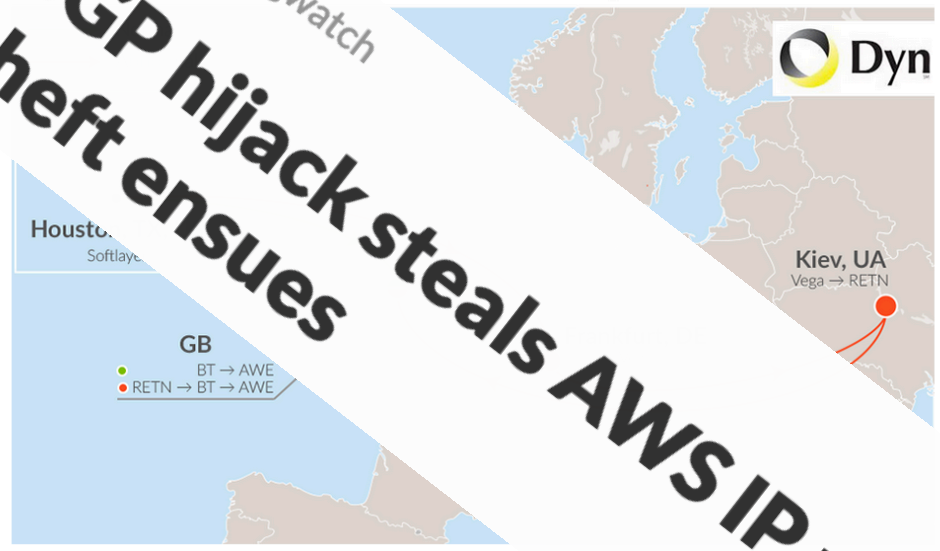
Security of core infrastructure

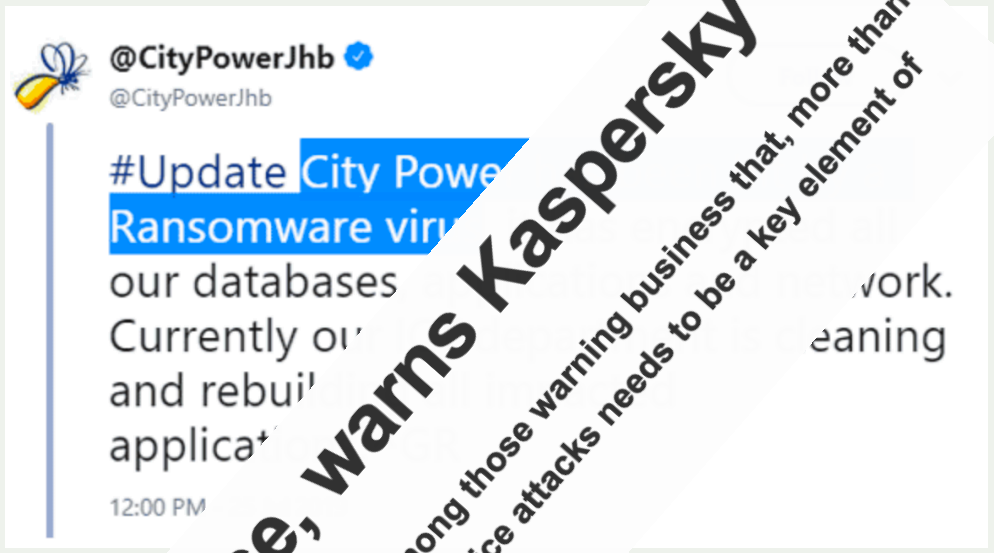
Massimiliano Stucchi

ITU Regional Event, Manama, October 1-3 2019

Security Blogwatch

BGP hijack steals AWS IP range; cryptocurrency theft ensues





n the rise, warns Kaspersky

ners at Kaspersky are among those warning business that, more than
f distributed denial of service attacks needs to be a key element of
ategies

Incidents are pretty common

- 2018 Routing Security Review
  - 12.6k incidents
    - 4.4% of all ASNs affected
      - 3k ASNs victims of at least one incident
      - 1.3k ASNs caused at least one incident

source: https://www.bgpstream.com/

The Internet used to be a safe place

- Many core protocols were designed when the internet was a small place

- Also, cryptography was an expensive exercise
  - Computers were much much slower

- Measures are being added on top of these protocols nowadays
  - DNSSEC, RPKI, other

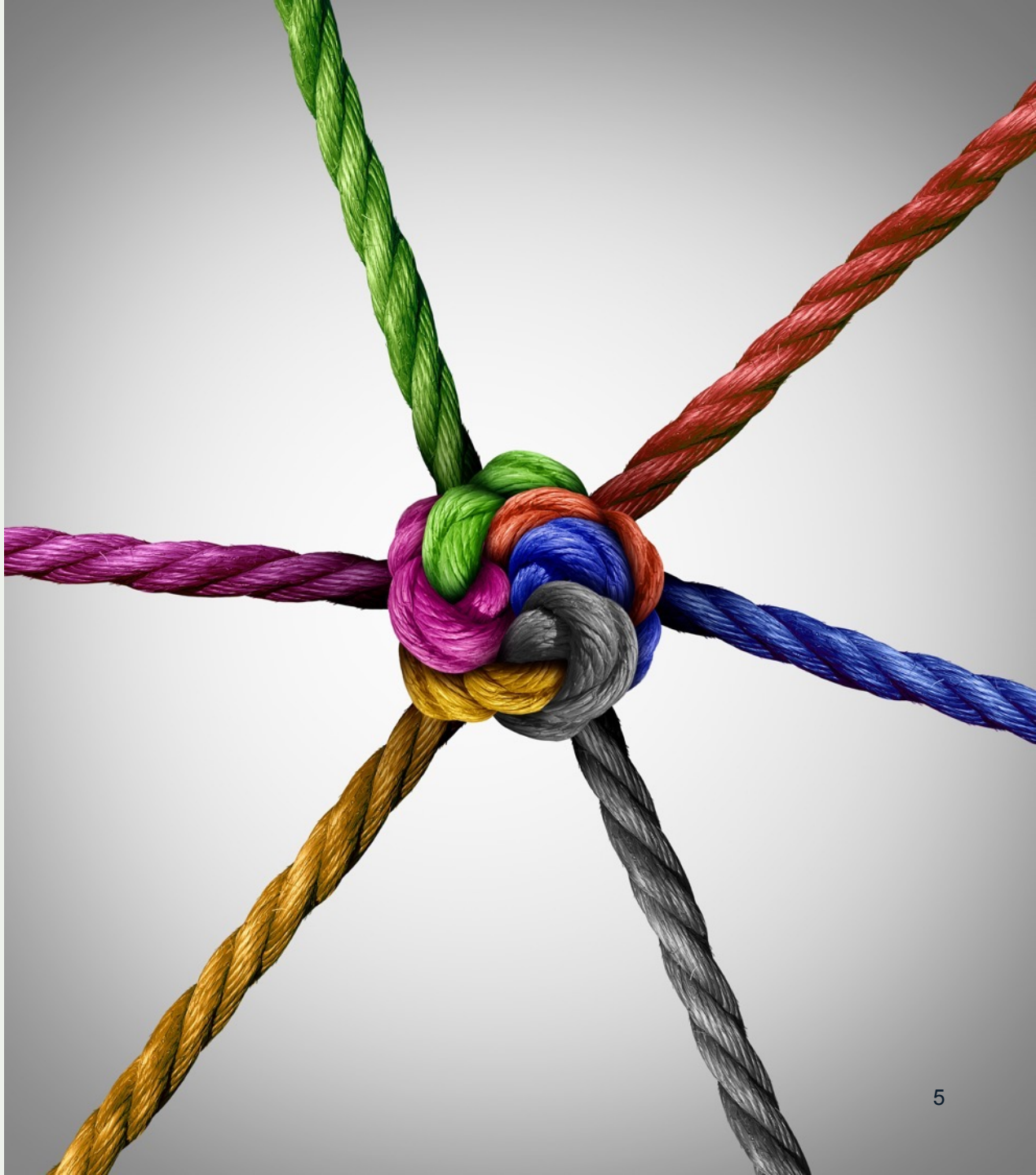
We Are In This Together

Network operators have a collective responsibility to ensure a globally robust and secure routing infrastructure.

Your network's safety depends on a routing infrastructure that mitigates incidents from bad actors and accidental misconfigurations that wreak havoc on the Internet.

Security of your network depends on measures taken by other operators.

The more network operators work together, the fewer incidents there will be, and the less damage they can do.



Mutually Agreed Norms for Routing Security

MANRS provides baseline recommendations in the form of Actions

- Distilled from common behaviours – BCPs, optimised for low cost and low risk of deployment
- With high potential of becoming norms

MANRS builds a visible community of security minded operators

- Social acceptance and peer pressure

MANRS

MANRS for Network operators

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible up-to-date contact information in common routing databases

Global Validation

Facilitate validation of routing information on a global scale

Publish your data, so others can validate

Questions ?

Thank you.

stucchi@isoc.org

@stucchimax

Quai de l'île 13
CH-1204 Geneva
Switzerland

11710 Plaza America
Drive Suite 400
Reston, VA 20190, USA

Rambla Republica de Mexico
6125
11000 Montevideo,
Uruguay

66 Centrepoint Drive
Nepean, Ontario, K2G 6J5
Canada

Sin El Fil, Dekwaneh Highway
Aramex Building, 2nd Floor
Beirut, Lebanon

Science Park 400
1098 XH Amsterdam
Netherlands

internetsociety.org
@internetsociety

9 Temasek Boulevard
#09-01 Suntec Tower Two
Singapore 038989