



BGP attack scenarios

Discussing BGP weaknesses



Andrea Dainese – CISO

- Senior Network & Security Architect with 15+ years' experience in securing complex IT and OT infrastructures
- Focused on cyber security strategies, GDPR/ISO27001 compliance and Automation
- Incident Response Team
- Cisco (CCIE), VMware, Red Hat... certified
- Father of Unified Networking Lab (UNetLab)
- Privacy and digital security evangelist – expert counselor-mediator in Cyberbullying

<https://adainese.it>



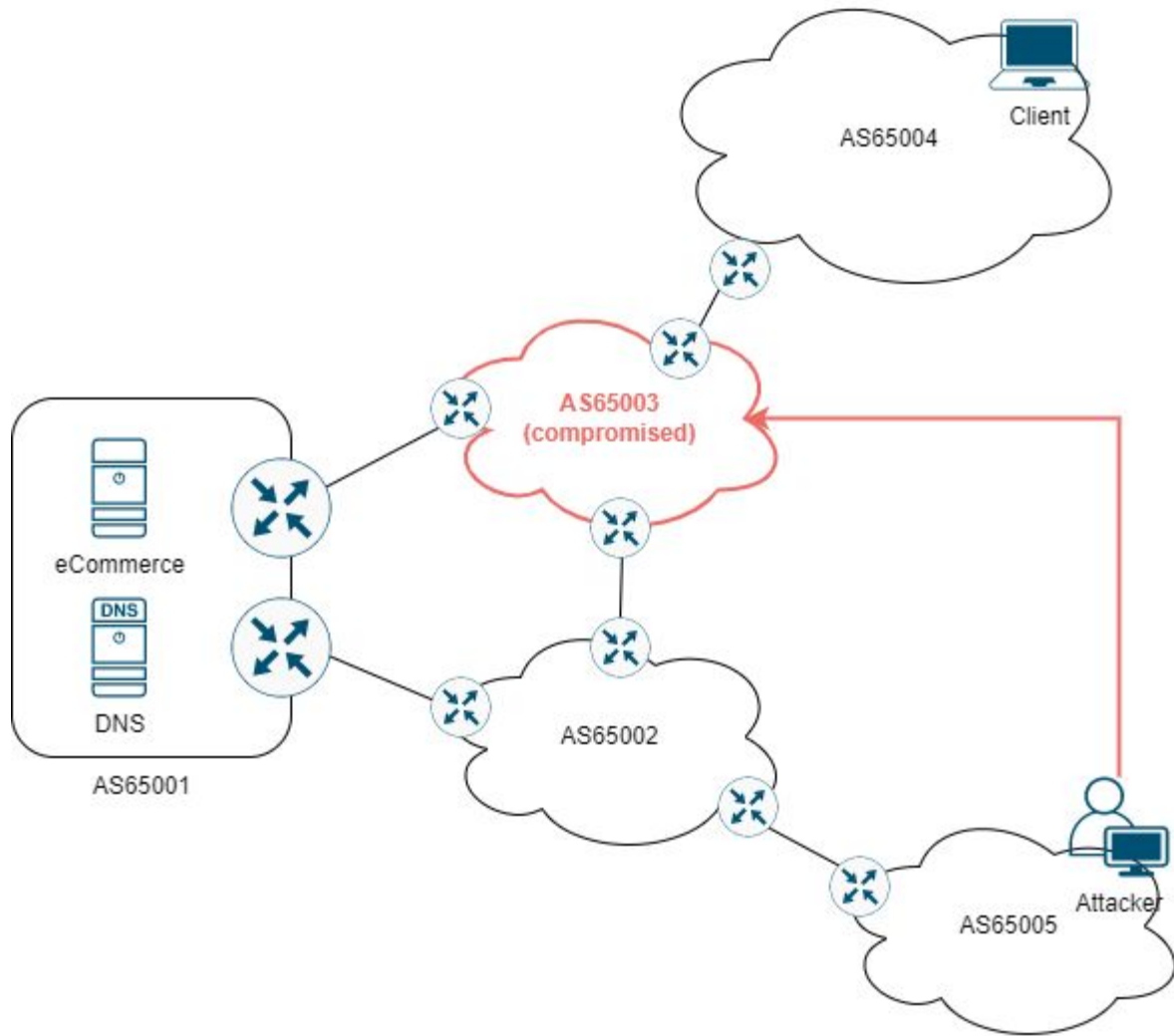
An aerial night view of a city with glowing traffic and network lines. The image features a blue color palette with white highlights. A network of glowing white arcs connects various points across the city, suggesting a data or communication network. The city lights and traffic are visible in the background, creating a sense of a busy, interconnected urban environment.

TRAFFIC INTERCEPTION





TRAFFIC INTERCEPTION



Traffic Interception / Man In The Middle (MITM)

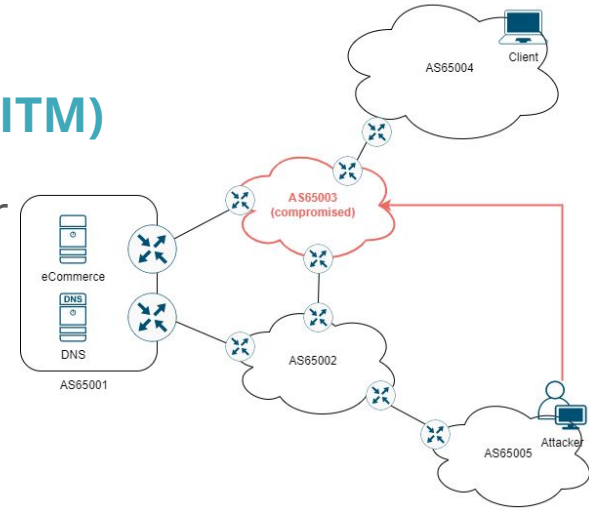
Attacker can announce black-holed prefixes or add flapping creating routing instability.

Impacts

- > Unencrypt traffic intercept

Mitigations

- > Hardening, auditing, certificate pinning (discouraged)
- > DNS security (marginally implemented <10%)



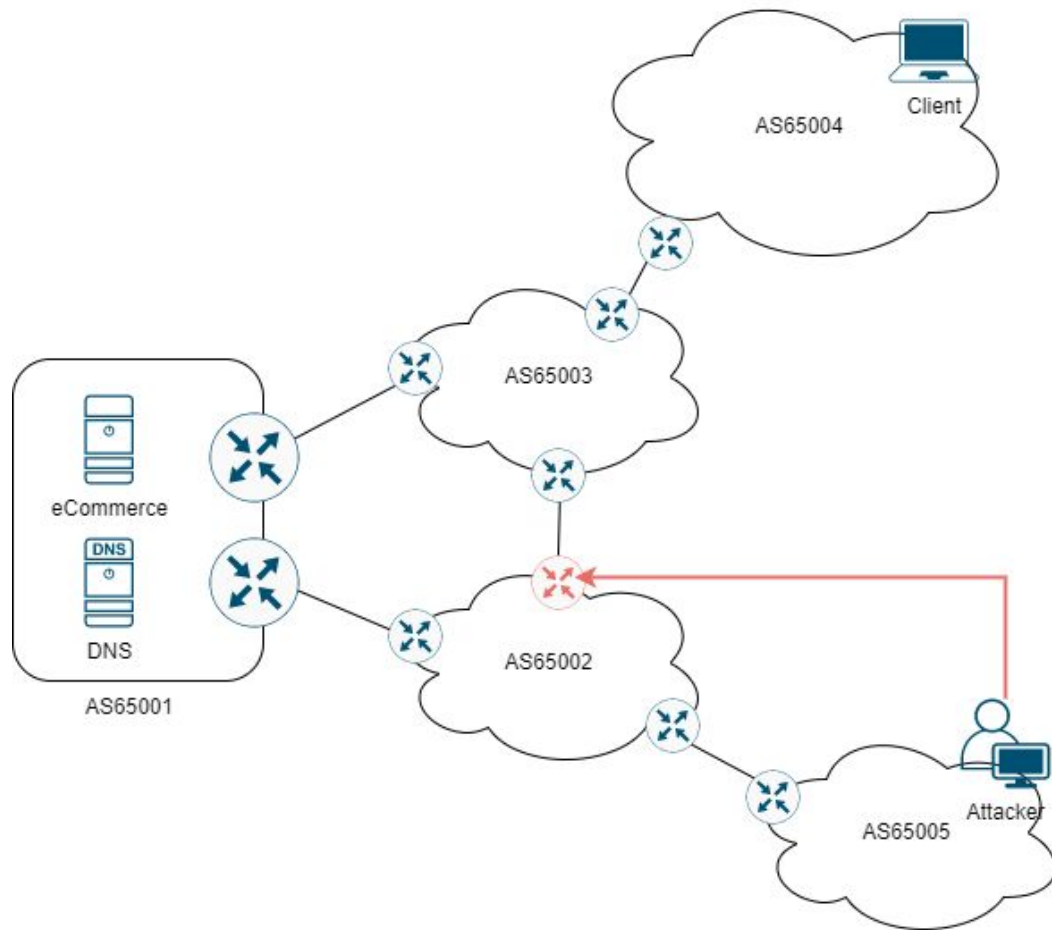
An aerial night view of a city, illuminated by city lights and streetlights. Overlaid on the city is a network diagram consisting of several glowing white nodes (dots) connected by thin, curved white lines (arcs). The nodes are positioned at various points across the city, and the arcs represent connections between them, creating a complex web of paths. The overall color scheme is a deep blue, with the city lights providing a contrast of white and yellow. The text "ROUTING INSTABILITY" is centered in the middle of the image in a bold, white, sans-serif font.

ROUTING INSTABILITY





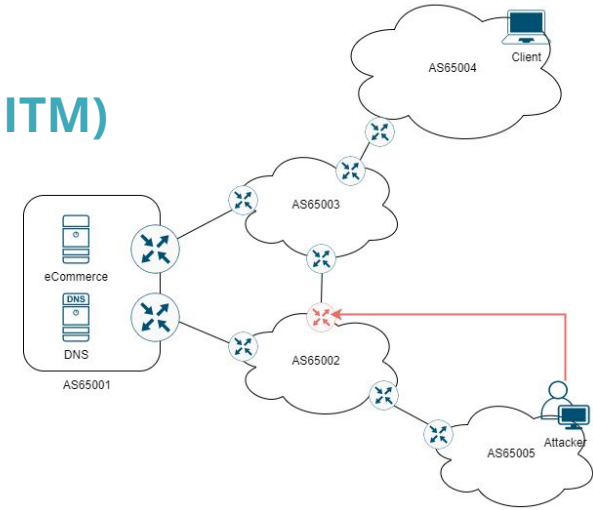
ROUTING INSTABILITY





Traffic Interception / Man In The Middle (MITM)

Attacker can intercept client-to-server traffic (via compromised router, compromised AS, bribery). Attack could compromise any router (server-side, transit-AS, any AS).



Impacts

- > Flapping network connections
- > Outage

Mitigations

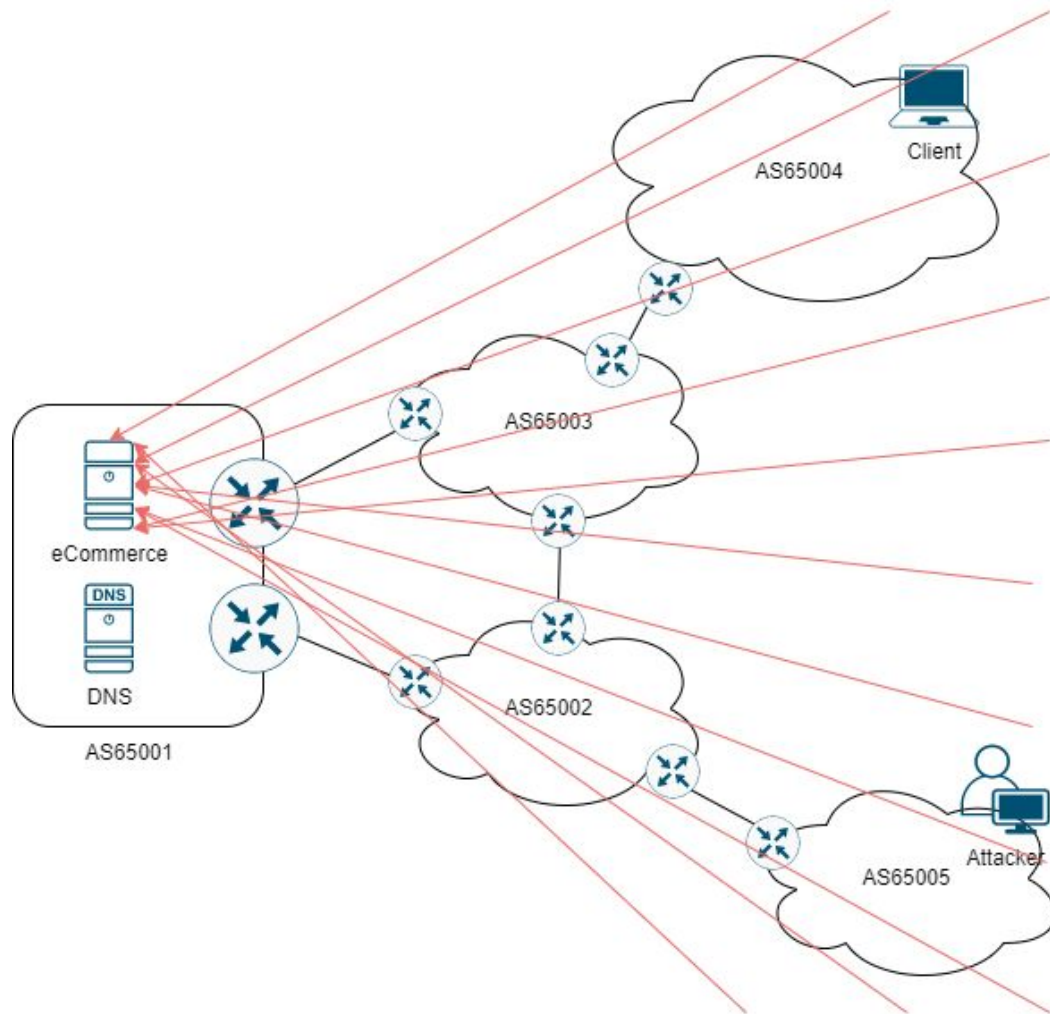
- > RPKI, hardening, auditing

An aerial night view of a city, likely Tokyo, with a complex network of glowing white arcs and nodes overlaid on the scene. The arcs connect various points across the city, suggesting a global or regional network. The city lights are visible in the background, and the overall color scheme is a deep blue with white highlights from the network and city lights.

DDOS / SOURCE DDOS



DDOS



Traffic Interception / Man In The Middle (MITM)

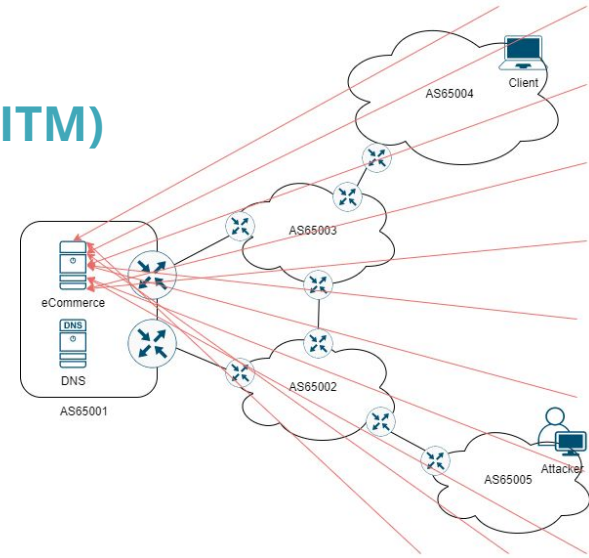
Attacker can orchestrate compromised clients to send data to a specific web service, consuming resources (CPU, memory, bandwidth).

Impacts

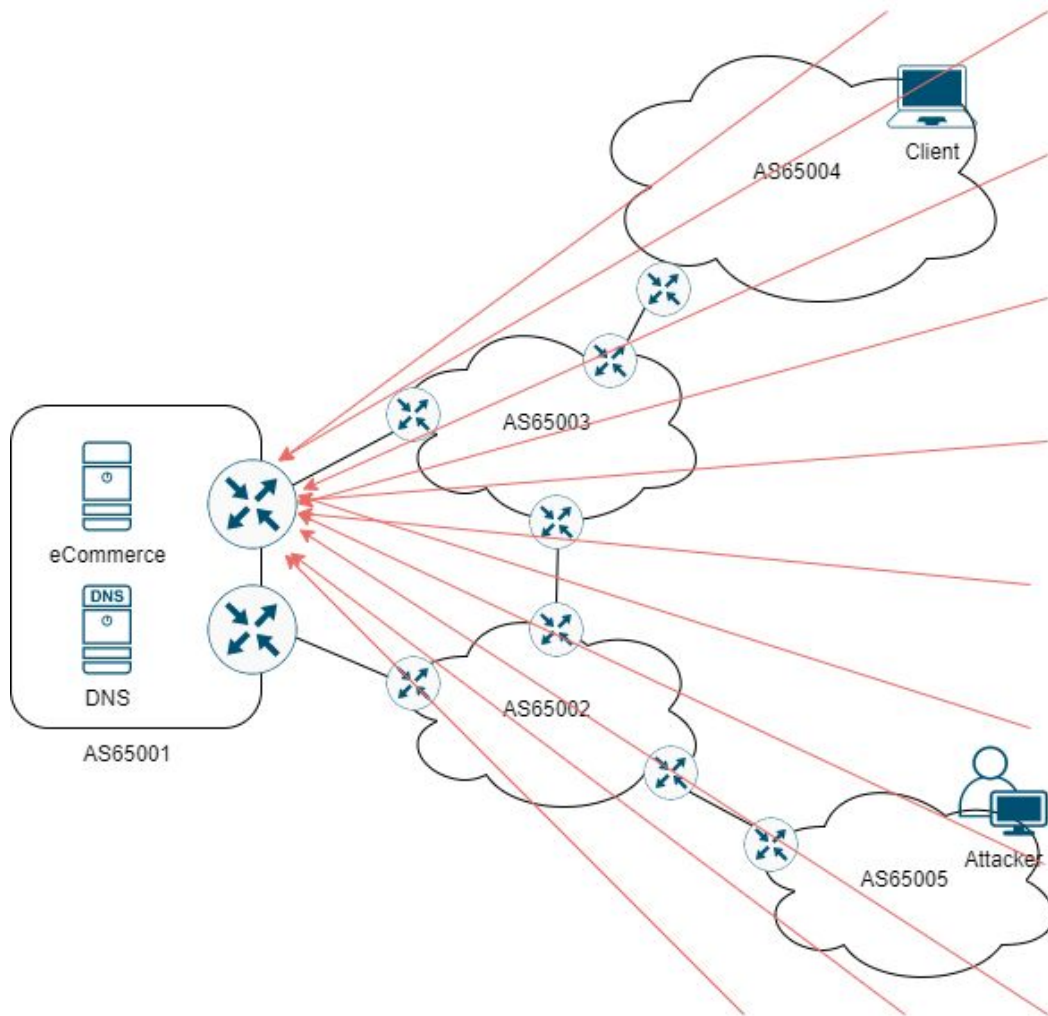
- > Outage

Mitigations

- > Anti DDOS (cloud-based)



DDOS



Traffic Interception / Man In The Middle (MITM)

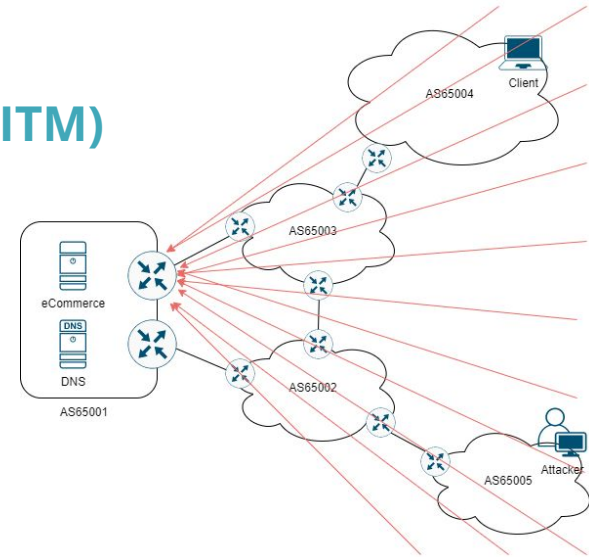
Attacker can orchestrate compromised clients to send data to a border router consuming resources (CPU, memory, bandwidth).

Impacts

- > Outage

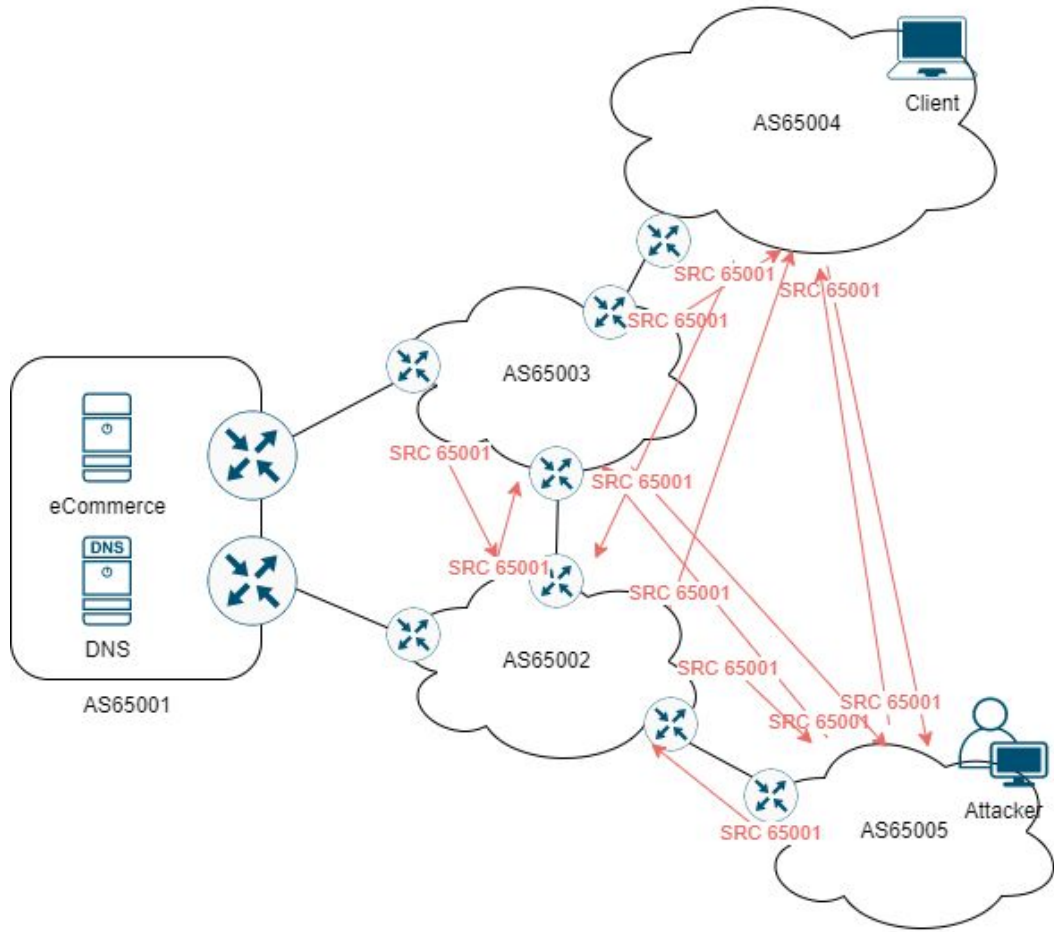
Mitigations

- > Anti-DDOS (ISP)



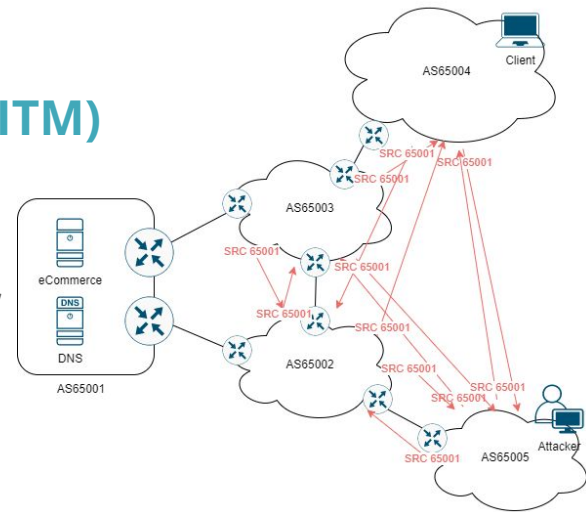


Indirect.DDOS



Traffic Interception / Man In The Middle (MITM)

Attacker can orchestrate compromised clients to send spoofed data to a specific web service, consuming resources (CPU, memory, bandwidth).



Impacts

- > Outage caused by blacklists

Mitigations

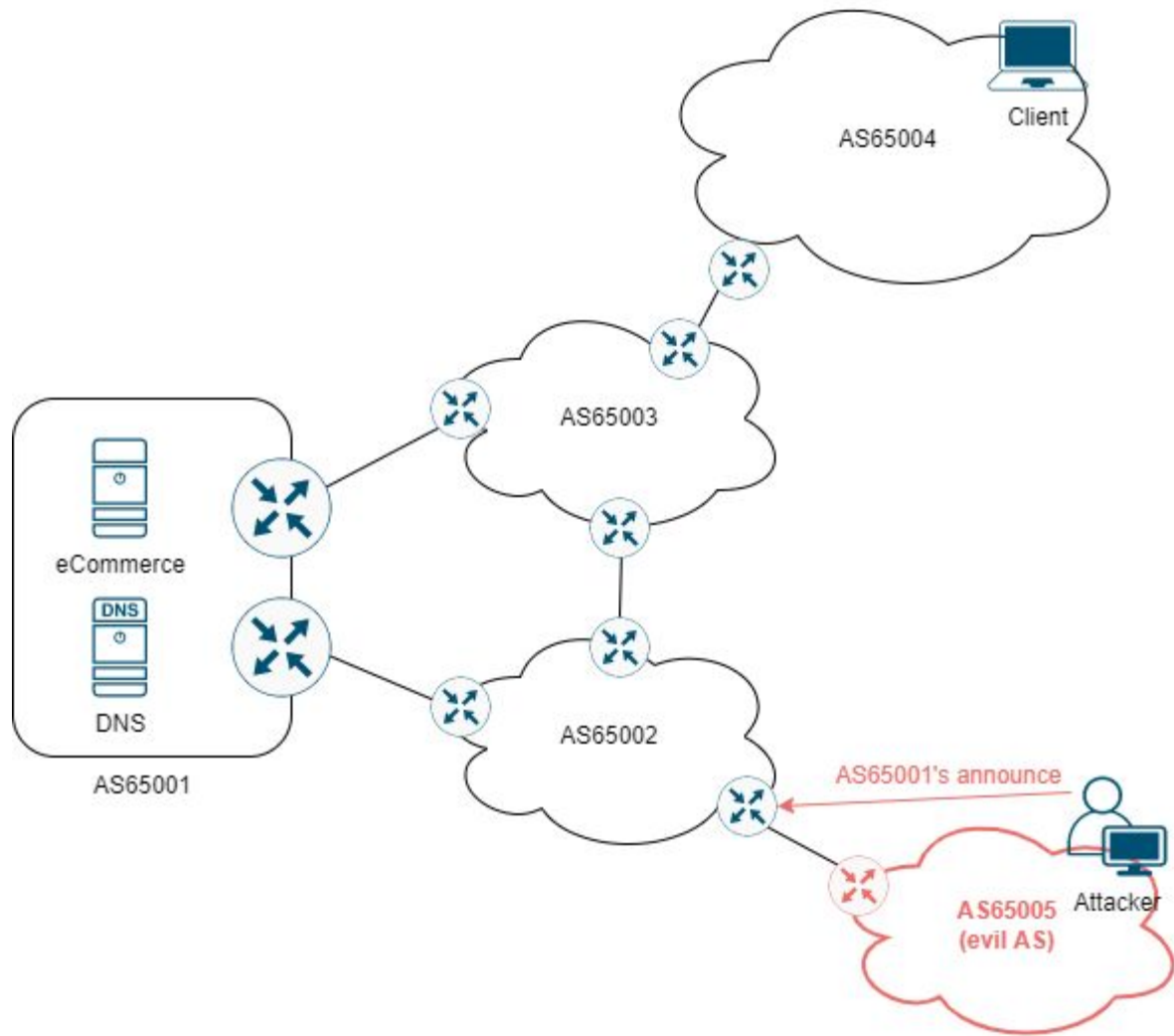
- > Traffic filtering (on customers' traffic)
- > RPF (Reverse Path Forwarding)

BGP HIJACKING

The image features a night-time aerial view of a city, with its lights and infrastructure visible. Overlaid on this scene is a network diagram consisting of several glowing blue nodes (small circles) connected by curved lines (arcs) that span across the city. The nodes are positioned at various points, some appearing to be on buildings or streetlights. The overall color scheme is a deep blue, with the city lights providing a contrast. The text 'BGP HIJACKING' is centered in the middle of the image in a bold, white, sans-serif font.



BGP HIJACKING





BGP hijacking

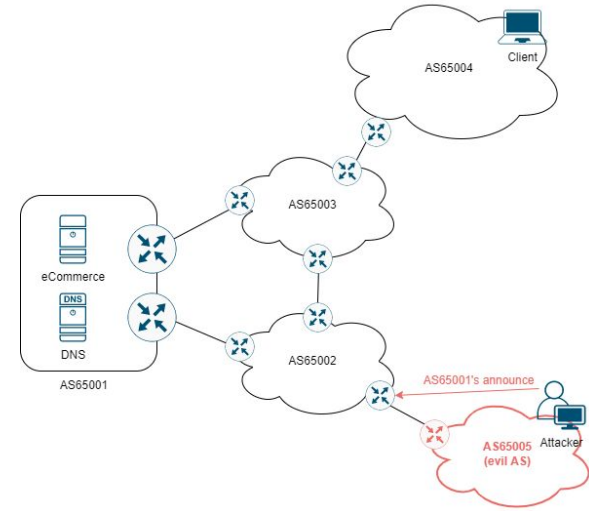
Attacker can announce AS65001's prefixes causing blackholes or fake services.

Impacts

- > Outage
- > PSK based VPNs are unaffected
- > TLS traffic authenticated via certificates can be affected (using Let's Encrypt services)

Mitigations

- > RPKI



An aerial night view of a city, likely Tokyo, with a complex network of glowing white arcs and nodes overlaid on the scene. The arcs represent connections between various points across the city, symbolizing a network or data flow. The city lights are visible in the background, and the overall color scheme is a deep blue with white highlights from the network and city lights.

RPKI VALIDATORS



Relying Party Software (as per 16/09/2022)

Name	Maintainer	Language	Last Commit	Version	Contributors
FORT Validator	NIC.mx	C	4 months ago	1.5.3 (11/2021)	12
OctoRPKI	Cloudflare*	Go	5 months ago	1.4.3 (02/2022)	16
rcynic	Dragon Research Labs	Python 2	9 months ago	?	4
Routinator	NLnet Labs	Rust	This month	0.11.3 (09/2022)	14
rpki-client	OpenBSD*	C	This month	7.8 (04/2022)	7
rpki-prover	Misha Puzanov	Haskell	1 month ago	0.3.3 (02/2022)	4
RPSTIR2	ZDNS	Go	3 month ago	?	3

<https://rpki.readthedocs.io/en/latest/ops/tools.html#doc-tools>



RTR Server Software (as per 16/09/2022)

OctoRPKI and rpki-client do not implement the RPKI-to-router (RTR) protocol, an external software is required.

Name	Maintainer	Language	Last Commit	Version	Contributors
GoRTR	Cloudflare	Go	22 months ago	0.14.7 (09/2020)	14
StayRTR	bgp	Go	2 months ago	?	18
RTRTR	NLnet Labs	Rust	This month	0.2.2 (06/2022)	4
rpkirtr	Darren O'Connor	Go	9 months ago	?	1



Security issues

- repositories are vulnerable to Denial of Service (DoS) attacks
- all implementations must make system calls to an rsync binary
- RPKI does not guarantee that the data is up to date

Recommendations

- RPKI Repository Delta Protocol or RRDP (RFC 8182)

rsync based security...

- It seems a little strange to build routing security on top of a protocol which we have demonstrated is inefficient, insecure and dangerous to run as server or client

An aerial night view of a city with glowing network lines overlaid. The city lights are visible in the background, and the network lines are represented by white arcs connecting various points across the city. The text is centered in the middle of the image.

**NETWORK EXPERTS
ARE NOT
SOFTWARE DEVELOPERS**





Recommendations

- › Routinator and one of FORT Validator or rpki-client + stayrtr
- › Prefer software included by default in Linux distributions
- › Be sure RPLI machines are included in asset/vulnerability/patch/lifecycle management processes
- › Force RRDP
- › Include it in your DR plan
- › Monitor them!!!

Mind that

- › Things rapidly change
- › Bugs (memory leak) also in “stable” versions
- › Reloading means re-validation (it’s a long process)
- › Managing Linux software is a system administration tasks

An aerial night view of a city, likely Tokyo, with a glowing blue network of arcs and nodes overlaid. The arcs connect various points across the city, suggesting a global or interconnected network. The city lights are visible in the background, and the overall color scheme is dominated by blue and white.

Q & A



An aerial night view of a city, likely Tokyo, with a glowing blue network overlay. The network consists of numerous bright white nodes connected by thin, glowing white arcs that curve across the cityscape. The city lights are visible in the background, and the overall color palette is dominated by deep blues and bright whites. The word "END" is centered in the image in a bold, white, sans-serif font.

END

