Nyx: Network Resiliency via Reactive Routing Decisions

Jared M. Smith and Max Schuchard
University of Tennessee, Knoxville

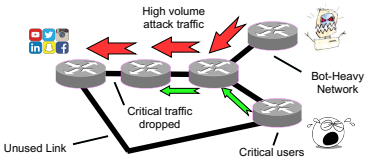
TICKLE COLLEGE OF ENGINEERING
THE UNIVERSITY OF TENNESSEE, KNOXVILLE

Abstract

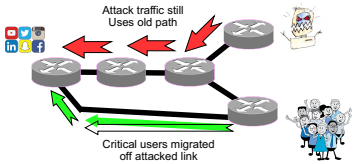
- DDoS attacks are on the rise and botnets have never been larger than they are today, yet current countermeasures can't stand up to the threat
- Links upstream of the victim Autonomous System (AS) become saturated by adversarial traffic and drop legitimate traffic
- We plan to mitigate this issue in two ways:
  - Load balance adversarial traffic across links inbound to the victim AS
  - Move legitimate traffic off saturated links around links impacted by DDoS
- In this work, we show we can accomplish the primitives required to do this by showing that an AS can manipulate traffic that is coming into it from an arbitrary AS on an arbitrary link

The Effects of DDoS Attacks and the Flexibility of the Routing Topology

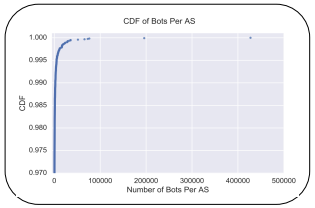
DDoS attacks saturate links and cause critical traffic to be dropped, but BGP is not aware of attacked links and doesn't attempt to preserve Quality of Service



Our system can manipulate routes so that critical traffic stays off attacked links while other links are under stress due to an attack



Bot Distribution in the Internet



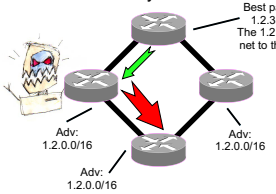
If we can move legitimate, non-bot traffic off the links that are along the best paths for those ASes, then we can halt the affects of DDoS attacks since there are a small number of ASes with a large amounts of bots

Impacting Incoming Traffic

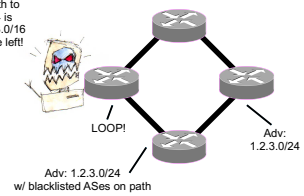
- Path selection decisions only control ***outbound*** traffic, not ***inbound***
- ***Fraudulent Route Reverse Poisoning*** (FRRP) uses BGP hole punching to reroute incoming traffic
  - BGP allows for sub-blocks of existing IP blocks to be advertised
  - Packets are forwarded along the best path to the *most specific* prefix known
  - Victim ASes, which we call reactor ASes, can falsely add all bot ASes to the BGP path of advertised routes as well as ASes along links they want incoming traffic to avoid, which we call moved ASes
  - Moved ASes will ignore these routes because of loop detection, and not propagate them

Fraudulent Route Reverse Poisoning

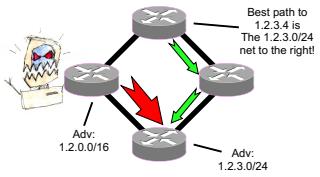
Non-reactors will send traffic bound to reactors across attacked links and links around bot heavy ASes



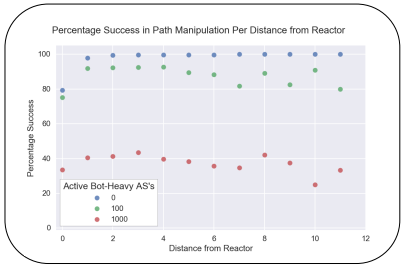
Reactors hole-punch routes adding blacklisted ASes, loop detection prevents route propagation



BGP will forward using the hole-punched route if available, which will not traverse over attacked links



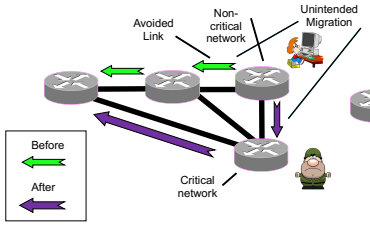
Percentage Success



Reverse Poisoning Side-Effects

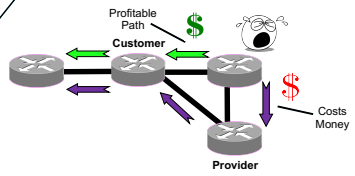
- By manipulating paths outside of the reactor AS, we cause several side effects to varying degrees:
- Disturbing other ASes best paths
  - **Problem**: We don't want to saturate additional links on critical paths to the reactor AS
- Changing the BGP Local Preference for routes
  - **Problem**: We don't want to incur additional monetary costs on ASes
  - Note: we don't observe this in our results
- Increasing the path length from reactor AS to other ASes
  - **Problem**: We don't want to lower performance of the network

We sometimes change the best paths to the reactor of ASes in the topology, which will be mitigated in future work

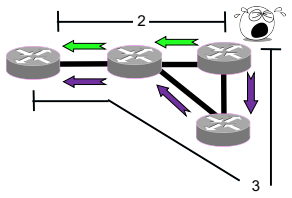


Side-Effects

We could cause inter-AS business relationships to change for routes, incurring financial costs on affected ASes

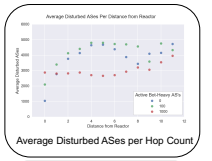


We sometimes cause path length increases from critical ASes to the victim AS, though modest at the most

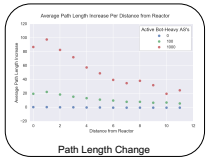


We did not see any monetary cost increases!

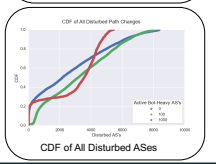
Side-Effects of Path Manipulation



Average Disturbed ASes per Hop Count



Path Length Change



CDF of All Disturbed ASes