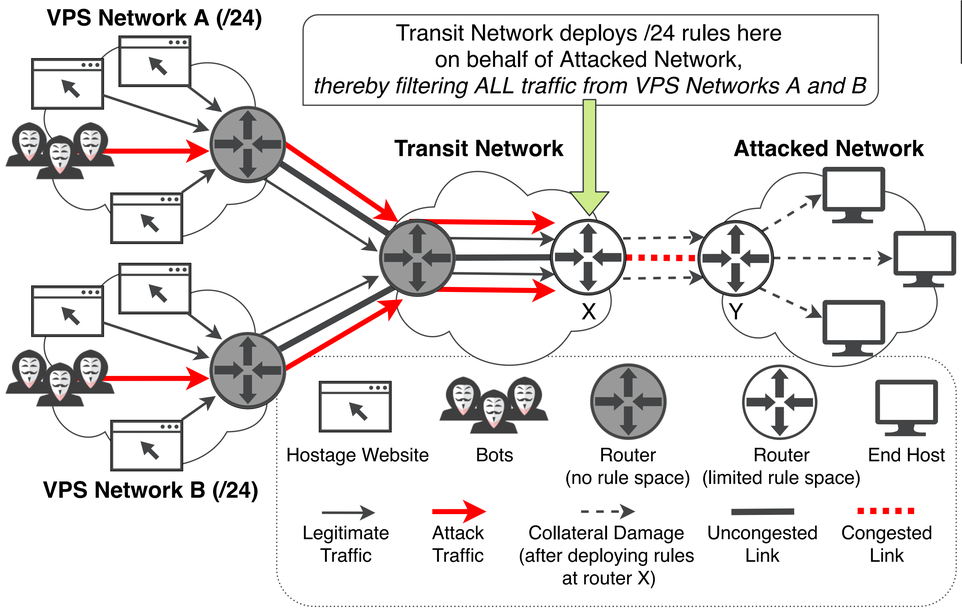
The Catch-22 Attack

Lumin Shi, Devkishen Sisodia, Mingwei Zhang, Jun Li, Alberto Dainotti, Peter Reiher

luminshi@cs.uoregon.edu, dsisodia@cs.uoregon.edu, mingwei@caida.org, lijun@cs.uoregon.edu, alberto@caida.org, reiher@cs.ucla.edu

ABSTRACT

- The Catch-22 attack is a distributed denial-of-service (DDoS) link-flooding attack that exploits real-world limitations of DDoS defense.
- An attacker leverages:
  - virtual private server (VPS) providers and residential proxy services as sources for assembling a botnet
  - moving target attack to maximize the amount of strain on DDoS defense, and
  - the collateral damage triggered by the DDoS defense of the attacked networks.
- With our preliminary evaluation, the attack can cause significant collateral damage to thousands of websites hosted at a major VPS provider.



BACKGROUND

- Today, websites and small networks often subscribe to DDoS protection services (DPSes) for DDoS defense.
- DPSes have finite bandwidth and computational capacity, and thereby cannot provide protection to all networks.
- For the remaining networks that are not protected by DPSes, the network community utilizes n-tuple traffic matching baked into modern IP routers for fine-grained DDoS filtering.
- Protocols such as BGP FlowSpec, allow networks to disseminate n-tuple filtering rules to their neighboring autonomous systems (Ases).
- Each router has a limited amount of high-speed memory (CAM/TCAM) in which filtering rules can be deployed.

THE CATCH-22 ATTACK

- The attack consists of two steps:
  1) Finding hostages: acquire bots that are co-located with the targeted hostages in a small subnet
  2) Moving target attack: attack multiple networks to increase the scale of the attack.
- Link-flooding attacks require victims to deploy filters in their upstream networks, e.g., router X in the figure above.
  - However, the attacked network may not be able to deploy rules on certain routers in upstream networks
  - The attacked network is forced to deploy coarsely granular source prefix rules (e.g., two /24 rules that filter all traffic from A and B) instead of finely granular individual IP rules (i.e., /32 rules that only filter the individual bots).
- The attack introduces a mitigation conundrum for the victims:
  1) Deploy fine-grained filters that incur no collateral damage but face ineffective DDoS mitigation
  2) Deploy coarse-grained filters to mitigate link-flooding attacks but face high collateral damage.

PRELIMINARY EVALUATION

- We conducted two experiments on two VPS providers to answer two obvious questions on server hostages.

1) Do VPS providers block potential outbound DDoS flows?
   - Ran large HTTP requests for an hour between two virtual machines (VMs), each located in a different VPS network.
   - No throughput degradation within a one-hour experiment period.
2) What server hostages can we possibly obtain?
   - Requested VMs from AWS and use each VM's /16 network prefix to mimic the effect of a large-scale attack.
   - Over 1,000 websites that are potential hostages using the 6 /16 network prefixes from AWS alone.
   - E.g., *deepai.org, uw.edu*, *xmind.net*, etc.

CONCLUSION

- We presented the Catch-22 attack, an imminent threat to today's Internet that can force attacked networks to cause large-scale collateral damage during DDoS defense.
- The Catch-22 attack is made possible due to the following limitations in real world defense:
  1) DPSes have finite filtering capacity, and
  2) inline mitigation depends on the scarce TCAM space available in today's networking devices.
- We plan to experiment with resources from VPS and residential proxy providers to quantify the attack damage.
- The core contribution of this work and its future extension is to examine fundamental vulnerabilities in today's DDoS defense infrastructure.