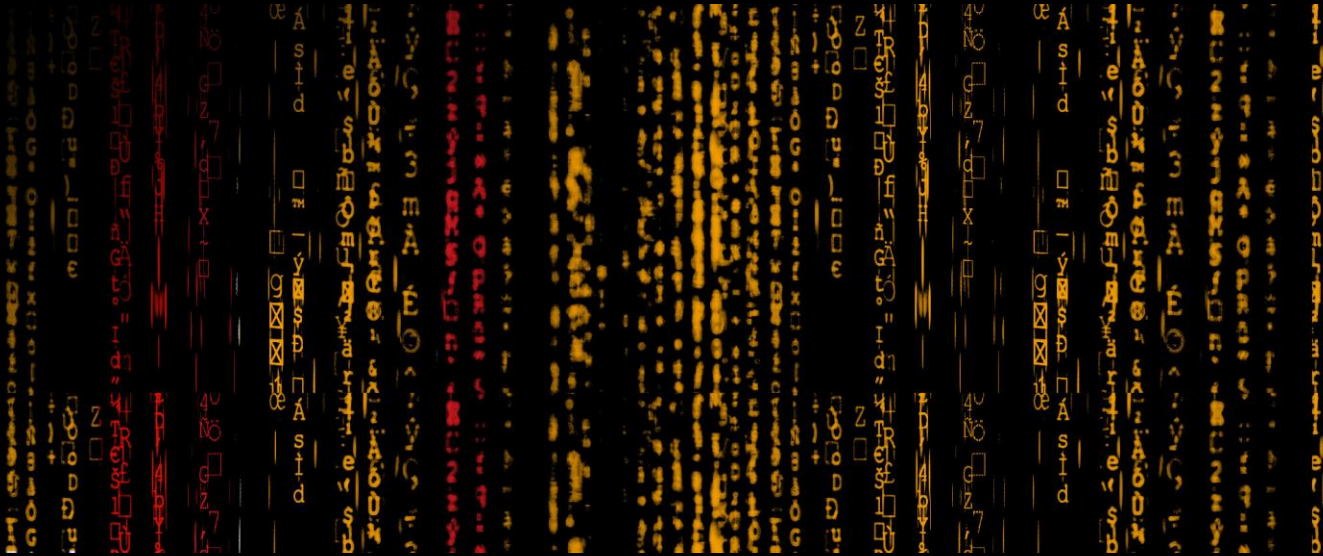
MMNOG

TEAM CYMRU

Team Cymru

Unwanted Traffic Removal Service (UTRS)

The “What/Why/How”



Tarek Sendi
Security Evangelist

AGENDA

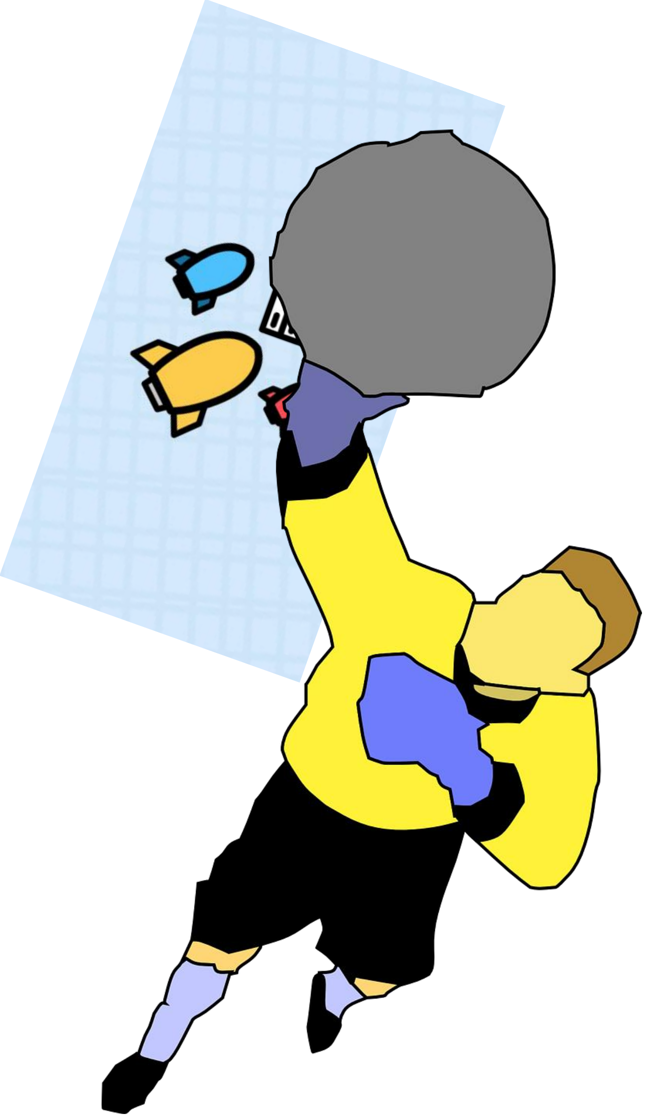
Introductions

Who is Team Cymru?

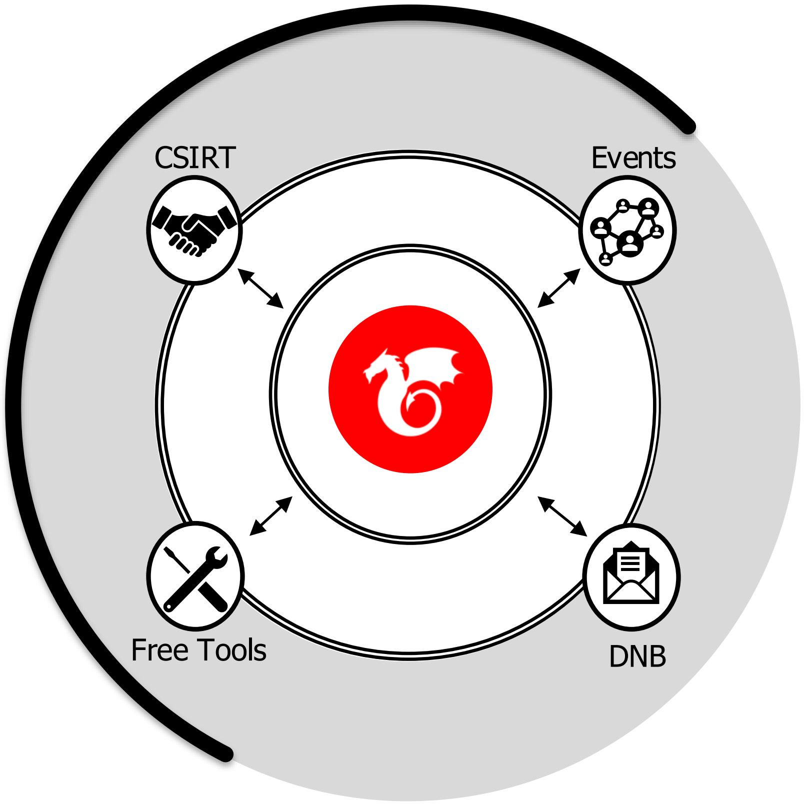
Overview of Community Services

UTRS™ (DDOS mitigation service)

- Tarek သည် မူလက တူနီးရှား CERT တွင် ဖြစ်ရပ်များ ကိုင်တွယ်သူအဖြစ် ဆိုက်ဘာလုံခြုံရေးတွင် သင်တန်းတက်ခဲ့ပြီး R&D တွင် အသင်းခေါင်းဆောင်ဖြစ်လာသည်။ "Team Cymru မှာ Tarek ဟာ အသုံးပြုသူတွေ၊ မိတ်ဖက်တွေနဲ့ ကျယ်ပြန့်တဲ့ လူ့အဖွဲ့အစည်းနဲ့ ဆက်သွယ်ဖို့ နေ့စဉ်အလုပ်လုပ်တယ်။ ကွန်ပျူတာမကြည့်ဘဲ အချိန်ကုန်ဆုံးနေတဲ့ တာရက်ဟာ ပန်းခြံထဲမှာ အလုပ်လုပ်နေပြီး ဘောလုံးပွဲတွေမှာ ဂိုးမသွင်းဖို့ အတတ်နိုင်ဆုံး ကြိုးစားနေတယ်။



Team Cymru



Who we Are

We uncover the who, what, when, where and why of malicious behavior.

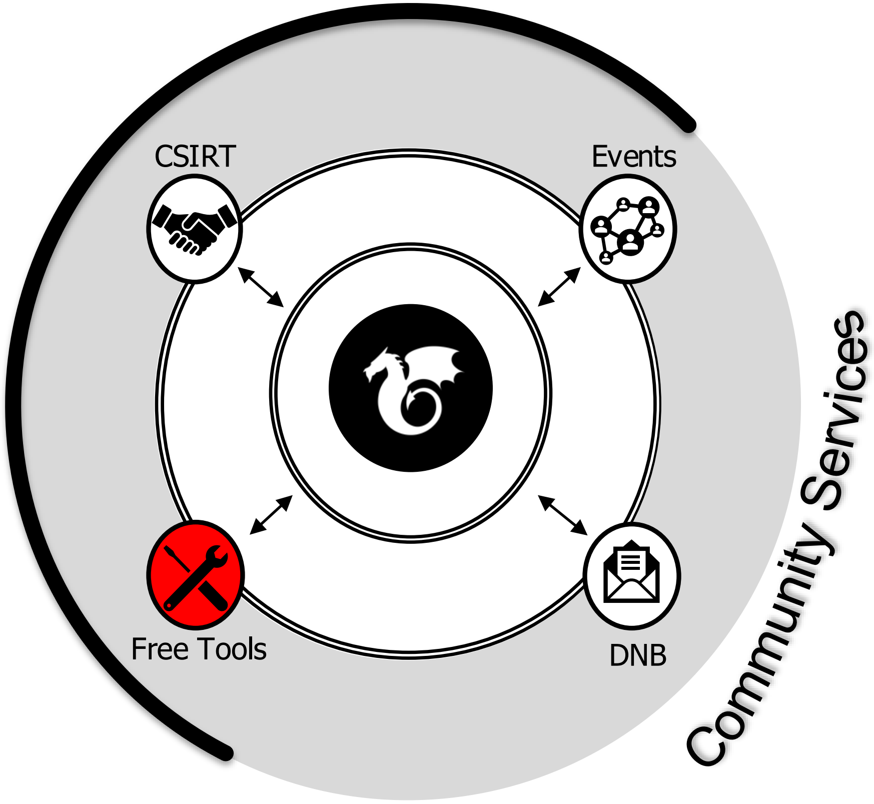
20+ years of service to network defenders, internet operators and cybercrime investigators worldwide.

- Free services for ISPs, hosting providers and CSIRTs
- Unmatched eco-system of data sharing and collaboration partnerships worldwide
- Work with 160+ CSIRT teams in 86+ countries
- Relied on by many security vendors, Fortune 100 companies, and public sector teams.

Team Cymru is comprised of former…

- Members of national and industry CSIRT teams
- Law enforcement
- Analysts from research, education, private and public sectors
- ISP backbone engineers

Outreach



Free Tools

Solutions provided by Team Cymru

Nimbus Threat Monitor: Kibana-based appliance that integrates our insight about malicious activity on your network, with near real time alerting

Unwanted Traffic Removal Service (UTRS): A system that helps mitigate large infrastructure attacks by leveraging an existing network of cooperating BGP speakers such as ISPs, hosting providers and educational institutions that automatically distributes verified BGP-based filter rules from victim to cooperating networks.

Bogon: Enhance Network Hygiene with Bogon Filtering
By filtering out Bogon IPs using our no cost Bogon Reference Community Service, you'll significantly reduce the risk of DDoS attacks and malicious traffic, ensuring a more robust and reliable network.

UTRS – Unwanted Traffic Removal Service (DDoS Mitigation Service)

UTRS Module Overview

- What is UTRS?
- What problem(s) are we helping to solve ?
- Requirements to signup for the UTRS Service.
- How to signup for the UTRS Service.
- How to implement UTRS Service on your network.
- Questions ?

What is UTRS ?

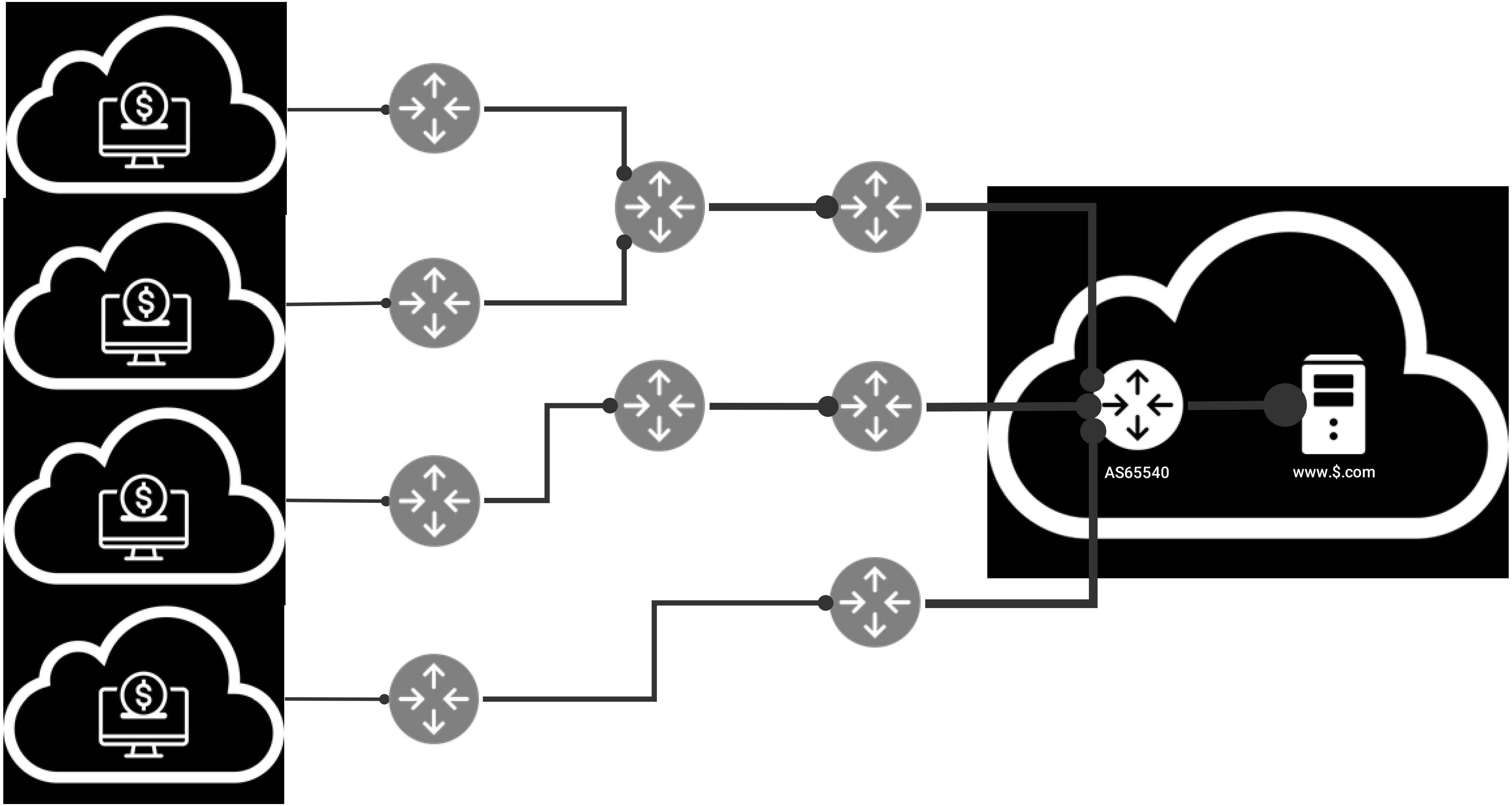
- UTRS == Unwanted Traffic Removal Service
- Fancy marketing name for “Community DDoS Mitigation”

What problem are we helping solve ?

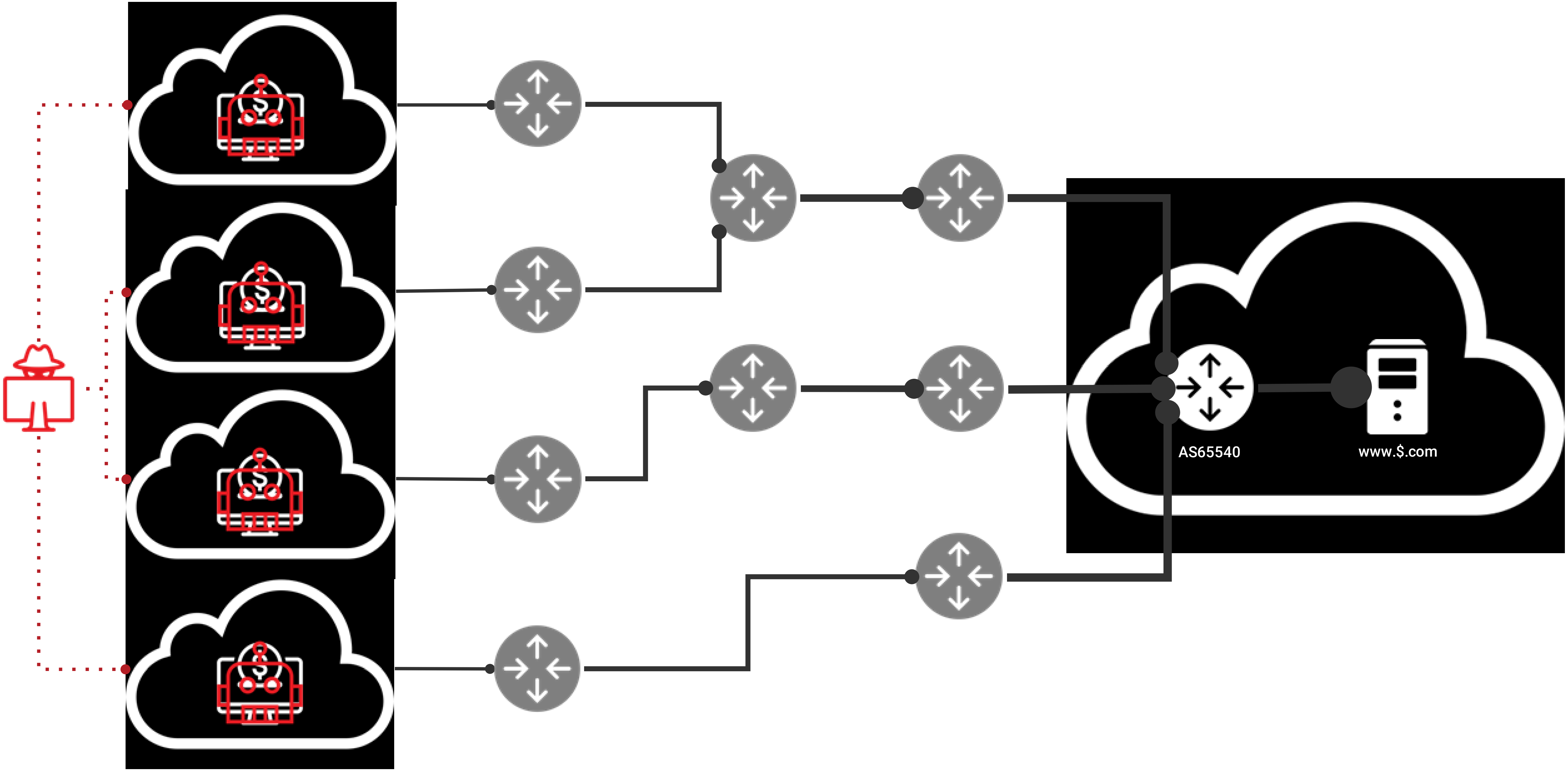
- Traditional DDoS mitigation works on filtering, scrubbing, dropping/blocking at the victim side.
- Team Cymru UTRS works by pushing the problem to the origination side. Let's stop the packets at their SOURCE!
- This helps save the entire internet

What is DDoS ?

- DDoS = Distributed Denial of Service.
  - It is an attack against one or more network resources designed to deny that resource from providing normal services.
- DDoS can be via an amplification attack.
  - Malicious actor sends a small flow of special packets towards a service that has a large response. Examples: Recursive DNS servers, NTP, CHARGEN and others.



AS65540
www.$.com

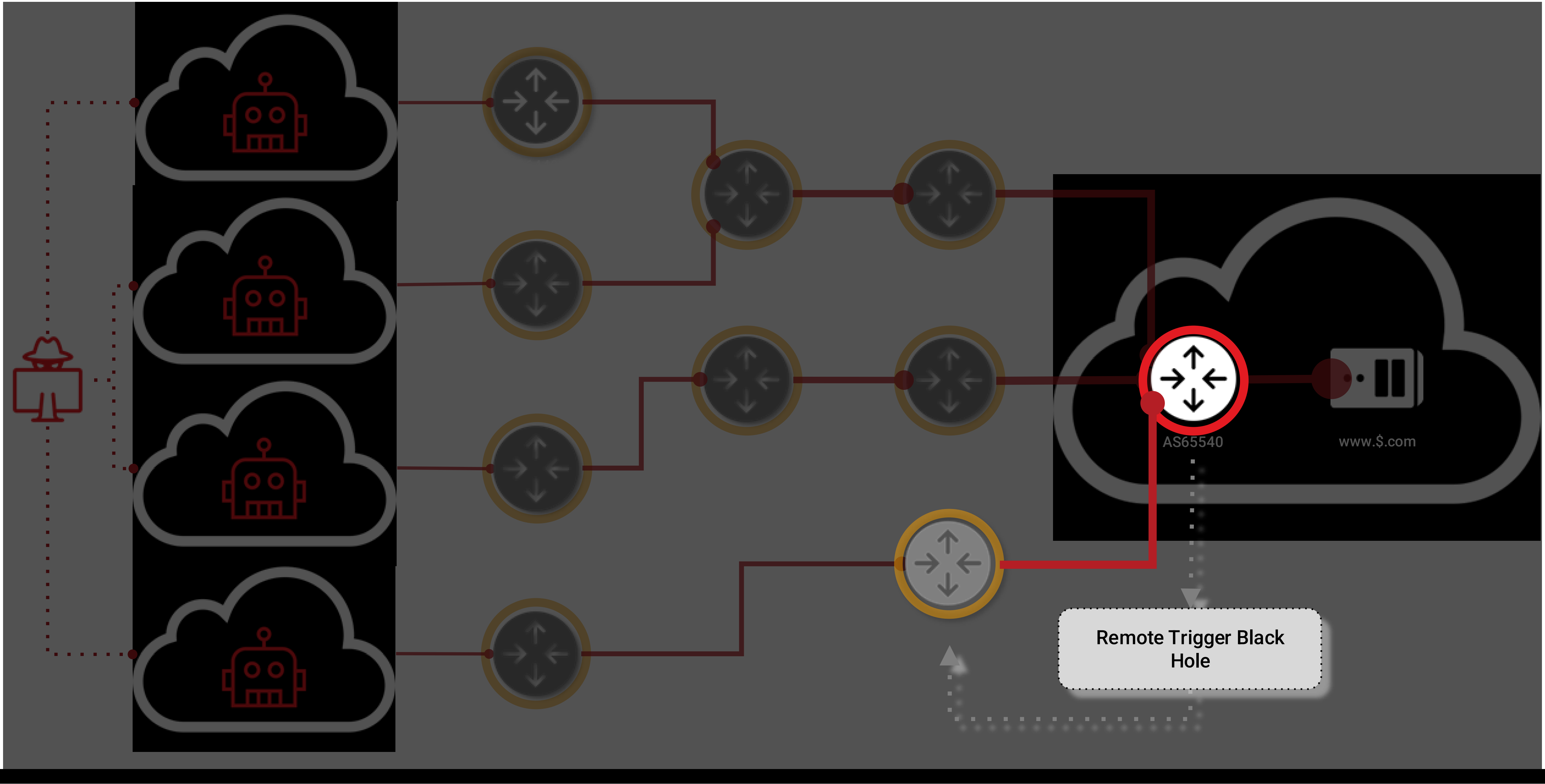

AS65540
www.$.com

How to mitigate, traditional methods.

- Traditional mitigation methods
  - Build an ACL (Access Control List) on your border router.
    - Doesn’t scale well across multiple border routers
    - Doesn’t scale well when there are hundreds or thousands of source IP’s
    - Your transit link is already congested, thus impacting more of your net.
  - Have someone else announce your routes and have them scrub / filter the traffic. This works when the vendor has bigger or more pipes than you do.

How to mitigate, the RTBH method

- RTBH (Remote Triggered BlackHole)
  - A special BGP session with your transit provider or peering partner
    - Using BGP to signal (tell them) your peer that you want them to drop traffic TO a specific address on your network.
    - Pushes the problem upstream. Your peer / transit is now absorbing the DDoS traffic. Hope their pipes are big enough to do that ☺!!
    - Works pretty good, you must build BGP sessions with each transit or peering partner. May not scale well..



Remote Trigger Black Hole

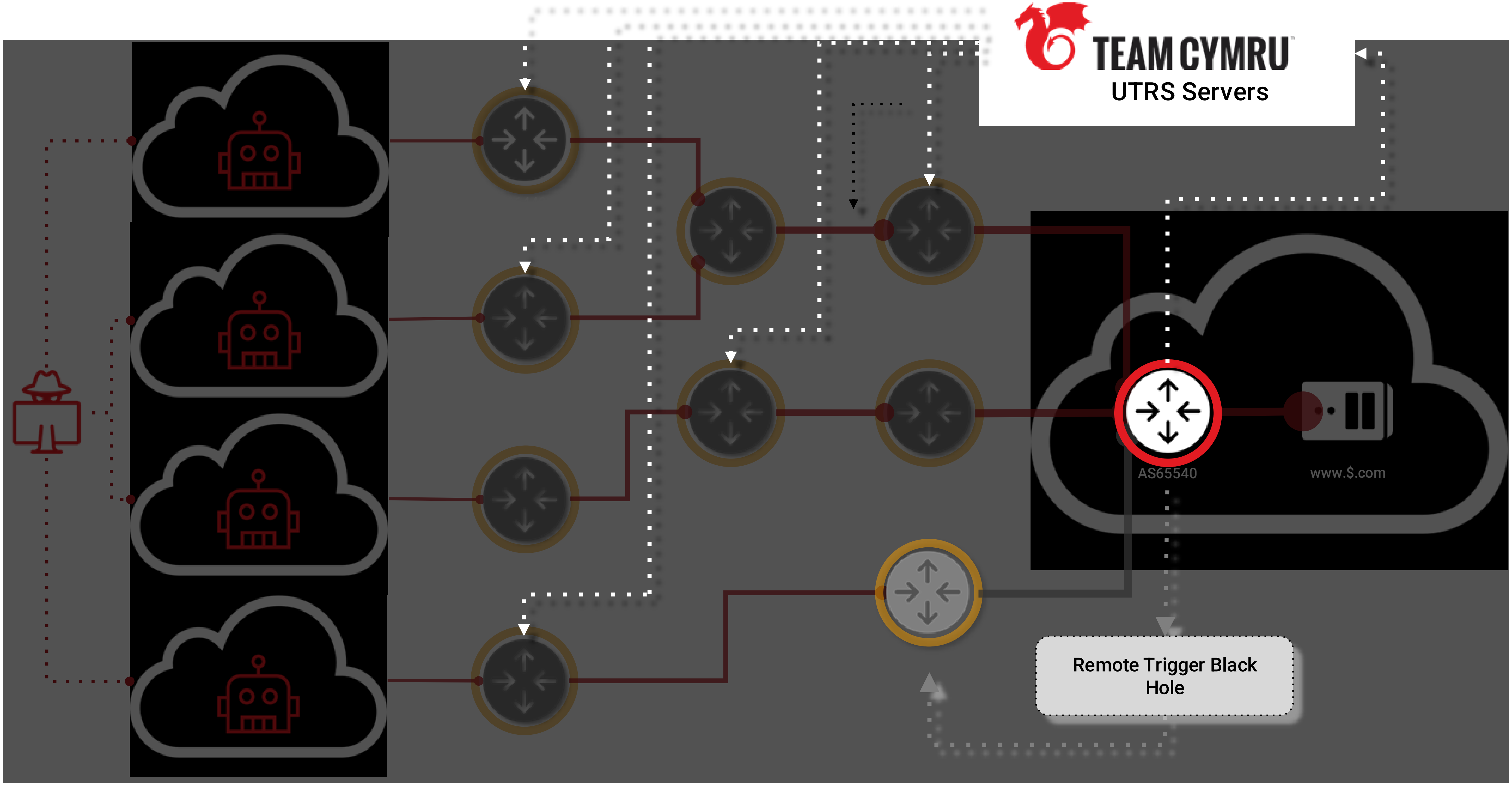
What if……..

We could tell more than 1000 networks to drop traffic we didn’t want

With only ONE BGP announcement!!

How to mitigate, the UTRS method

- UTRS == Unwanted Traffic Removal Service
  - Uses RTBH methods, but at scale
  - Team Cymru as a trusted partner, receives your request to drop traffic
  - TC validates the request
  - TC then sends the request out to the thousands of other UTRS members
  - Nearly instantly your traffic is being dropped as far upstream as possible


TEAM CYMRU
UTRS Servers
AS65540
www.$.com
Remote Trigger Black Hole

What is new UTRS 2.0

- Based on community feedback, Team Cymru has added new features:
  - Increase the prefix size from IPv4 /32 to IPv4 /25
  - Redundant Route Servers, geographically diverse, better peering
  - IPv6 support. We will now accept IPv6 up to a /49
  - Flowspec
  - RPKI Validation

What is new UTRS 2.0

- Increase the prefix size from IPv4 /32 to IPv4 /25
  - By allowing larger IPv4 prefixes we help prevent “carpet bombing”
  - Aligns better with route acceptance boundaries

What is new UTRS 2.0

- Redundant Route Servers
  - Many partners require two or more peering locations.
  - Partners also require geographically diverse locations
  - Increases redundancy, which increases reliability of service.

What is new UTRS 2.0

- IPv6 support
  - Most DDOS has been via IPv4 networks
  - IPv6 is growing and in some parts of the world will be dominate soon.
  - We now accept IPv6 prefixes up to a /49

What is new UTRS 2.0

- Flowspec
  - Allows for a more refined “surgical” removal of unwanted traffic
  - Flowspec rules MUST
    - Have a destination CIDR in the rule
    - Set action to DROP
  - Flowspec rules MAY
    - provide SRC/DST port (explicit, no ranges),
    - Protocol (TCP, UDP, etc)

What is new UTRS 2.0

- RPKI Validation
  - We will validate based on RIR information
  - By using digital signatures, we further validate the authority of the prefix.

Requirements to signup for UTRS

- You must have a valid public ASN (Autonomous System Number) as assigned by your RIR (Regional Internet Registry)
- You must be running BGP on your border / edge router
- You must submit to Team Cymru the prefixes you own and may announce for validation, Before you can use them.
- You must be willing and able to accept BGP requests via UTRS and then drop traffic going TO those addresses.

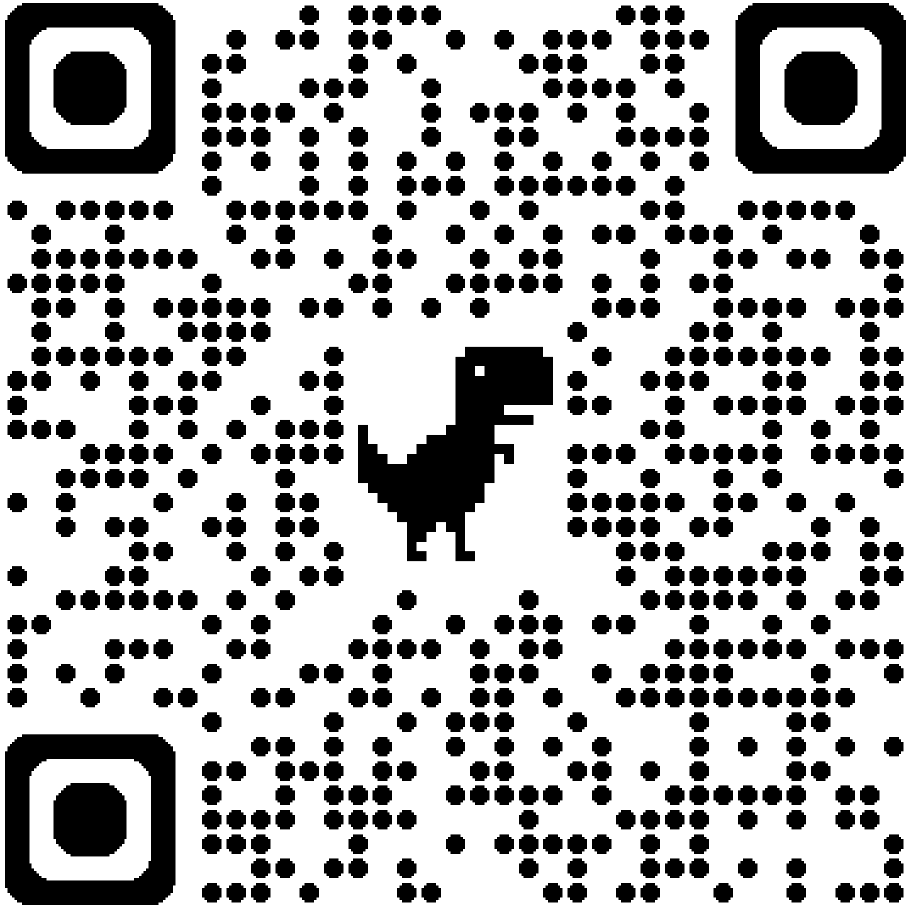
How to signup for UTRS

- Signing up for UTRS is easy, go to the following web address

  https://www.team-cymru.com/ddos-mitigation-utrs-services

- You will need to complete the form with the following info:
  - Your Name
  - Your Email address
  - Your company name
  - Your Public ASN
  - The IP address you will peer from
- We will then validate the information and send you details via email.

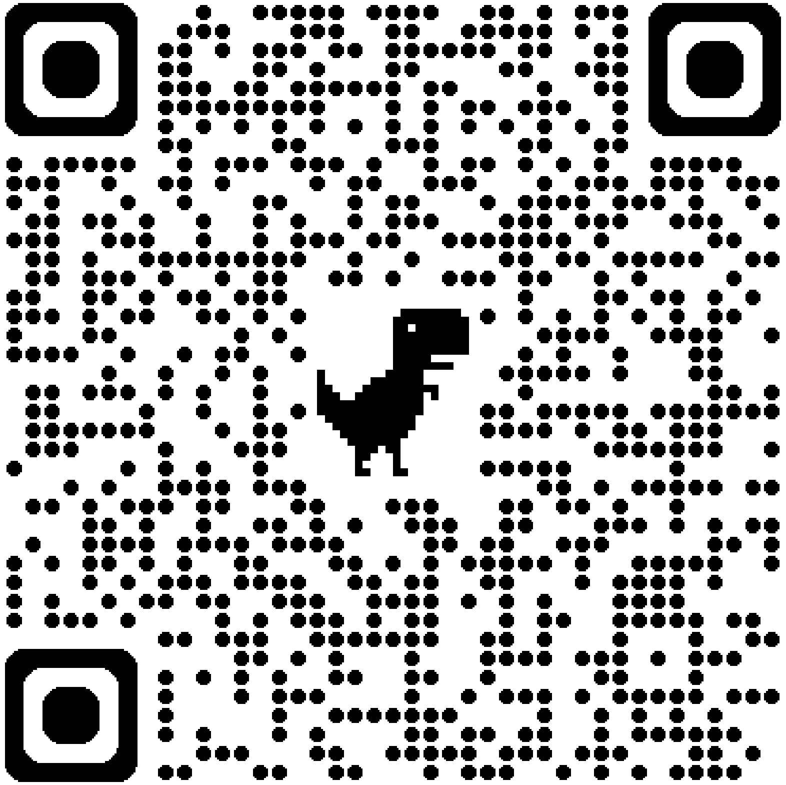
How to signup for UTRS



How to implement UTRS in your network

- Implementing UTRS is straight forward. Basically you:
  - Create a BGP neighbor / peer on your router with the info we provide
  - Build a route-map / policy-map that tags UTRS learned routes
  - Create a rule that discards traffic being sent to those tagged routes
- If you are a victim and need traffic removed by others, then:
  - You will create an announcement that contains the victim IP
  - This will be announced towards the UTRS service
  - Our automation will validate the announcement and then forward to others.
- We have lots of examples on our website / git-hub

How to implement UTRS in your network



QUESTIONS ?