DDoS Suppression

Industry actively suppressing the sources of DDoS & and enabling backtracking to the attacker source.

Barry Greene
bgreene@senki.org

1. Since 2021, the industry has been pushing back on DDoS Miscreants.
2. We have found ways to persistently poke the DDoS Miscreants.
3. Our community is growing. All it takes is 30 minutes a week, deploy the basics of network security, and have a security rhythm to maintain your network.

The industry was stuck ….

2019 our DDoS problem was increasing …..

- Miscreants were using the easiest DDoS vector - DDoS Reflection Attacks.
- We were not pushing back against these DDoS Miscreants.
- Boot/Stressor operations was making it easy for any miscreant to “outsource” or “pay” for attacks.
- The cost economics were skewed in the wrong direction.

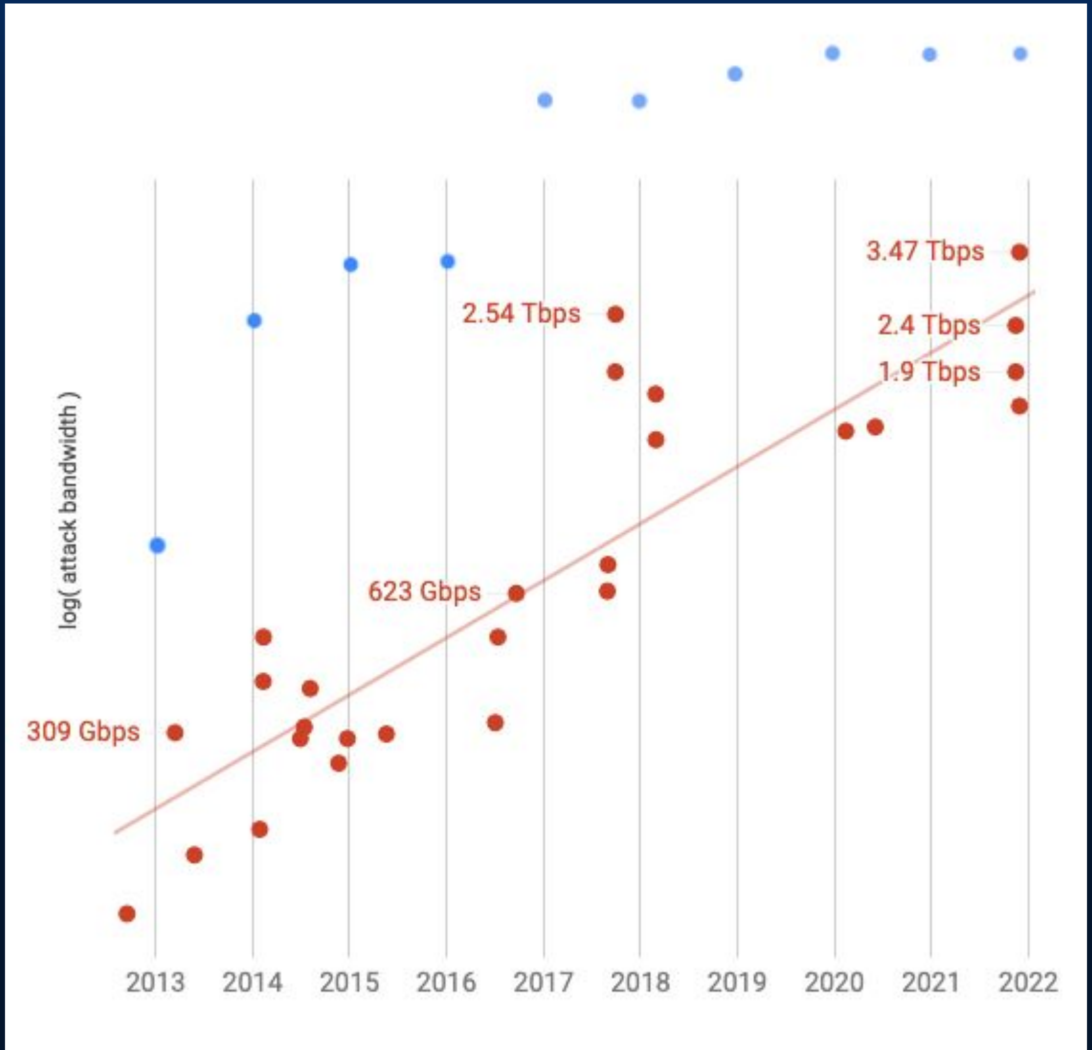
How bad can it get?

We've seen with the Weaponizing Middleboxes for TCP Reflected Amplification threat, the problem is not going away.

The 20% rule will continue. The % of security risk on IoT devices will increase. (see *1 Yottabyte DDoS Attack – The Biggest DDoS Attack in History!*)

The only thing saving the industry today is the miscreants taking the *easy path.* Easy DDoS Reflectors using Booter/Stressors, no vertical targeting (moving upstream to the ISP), no in-depth homework into the DDoS solution architecture, and no pressure from law enforcement.

Q. Do we really want to remain in this trap of a DDoS arms race?



Source: Damian Menscher (Google data) with Akamai PLX mitigation capacity in blue

How bad can it get?

Left unchecked, the DDoS criminal threat actors will:

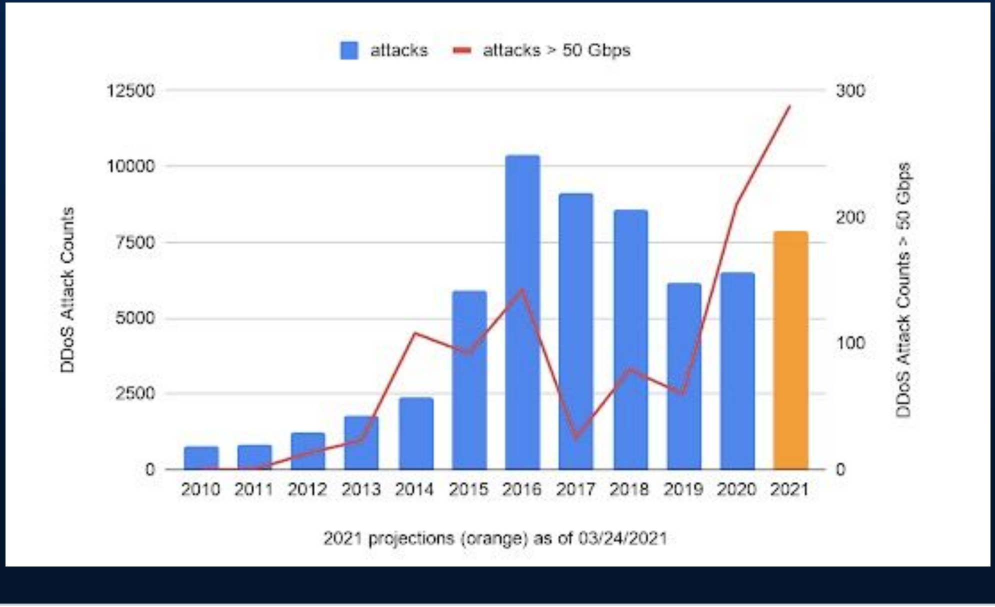
- Expand their DDoS tools
- Optimize their criminal enterprise (don't work too hard)
- Have redundancy to their operations
- Be mindful of their ROI - don't work too hard - move on if the defensive capabilities takes too much time. Criminal TAM is large, pivot quick and move to the next is a common behavior.
- Maintain their DDoS capacity to match the target's defensive capabilities. There has been an arms race.
- The "20%," massive infections, and poor product security means the DDoS Criminal will always have the upper hand … if left unchecked.

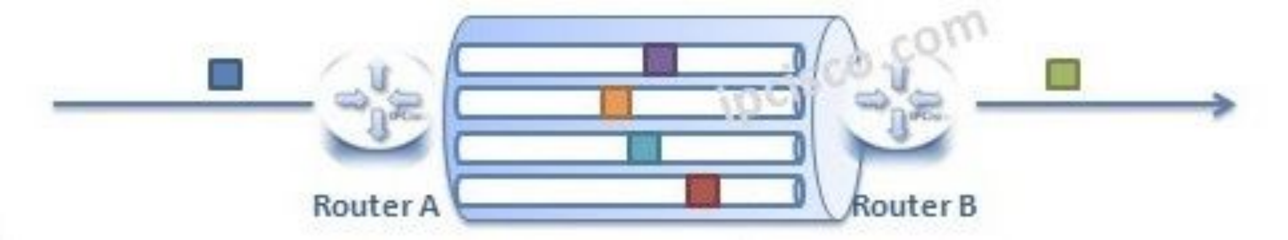
We cannot ignore the potential fire! We have to realize how bad it could get. A persistent DDoS Threat-Actor has a powerful range of tools. Left unchecked …… we can understand the risk.

Our 50G Problem

“We've had more +50G attacks (on PLX) in the Q1 2021 than in all of 2020.”

… and we have no understanding why ….



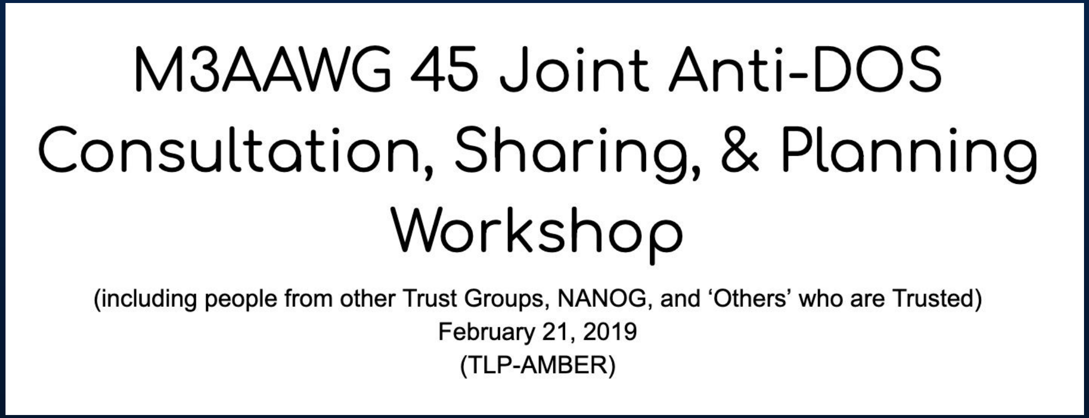


DANGER! 50G is at the range where an elephant flow will disrupt a 4x100G MLPPP backbone link (depending on the router, configuration, line cards, and fiber condition)

Meaningful & Actionable Consultation

An invitation only TLP: AMBER side workshop was held with as many of the key anti-DDoS participants as was possible.

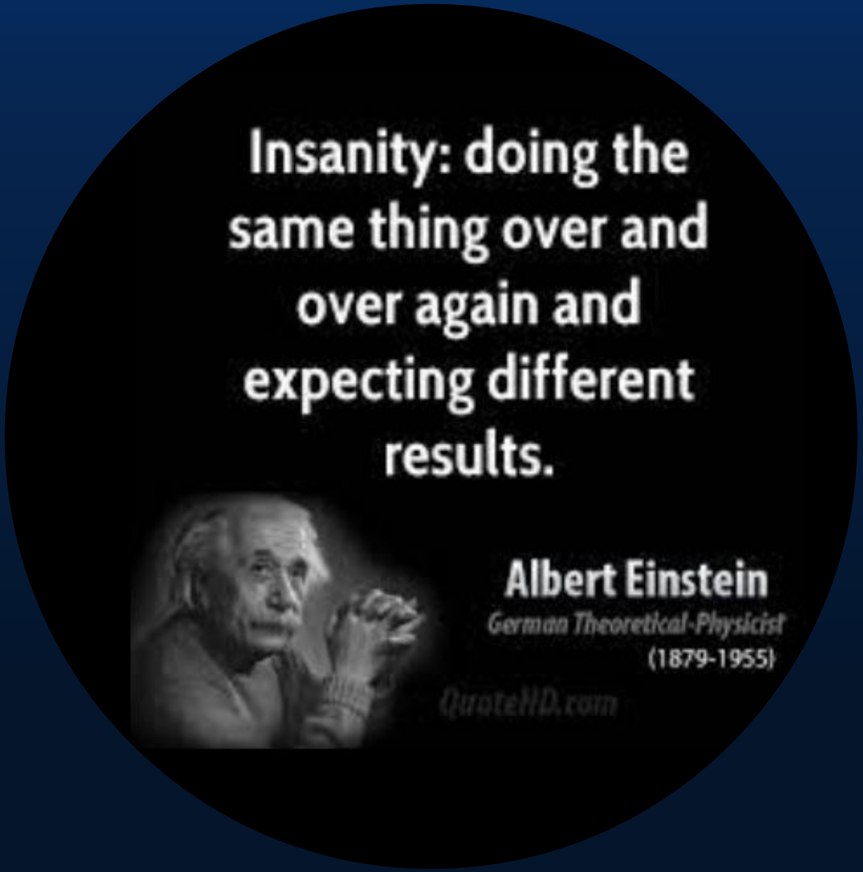
- That consultation explored all the various options.
- Ideation of how we would go about action took close to a year to evolve.
- The end result was a shift if how we responded to DDoS as a community.



M3AAWG 45 Joint Anti-DOS Consultation, Sharing, & Planning Workshop

(including people from other Trust Groups, NANOG, and 'Others' who are Trusted)
February 21, 2019
(TLP-AMBER)

Lets try something different!



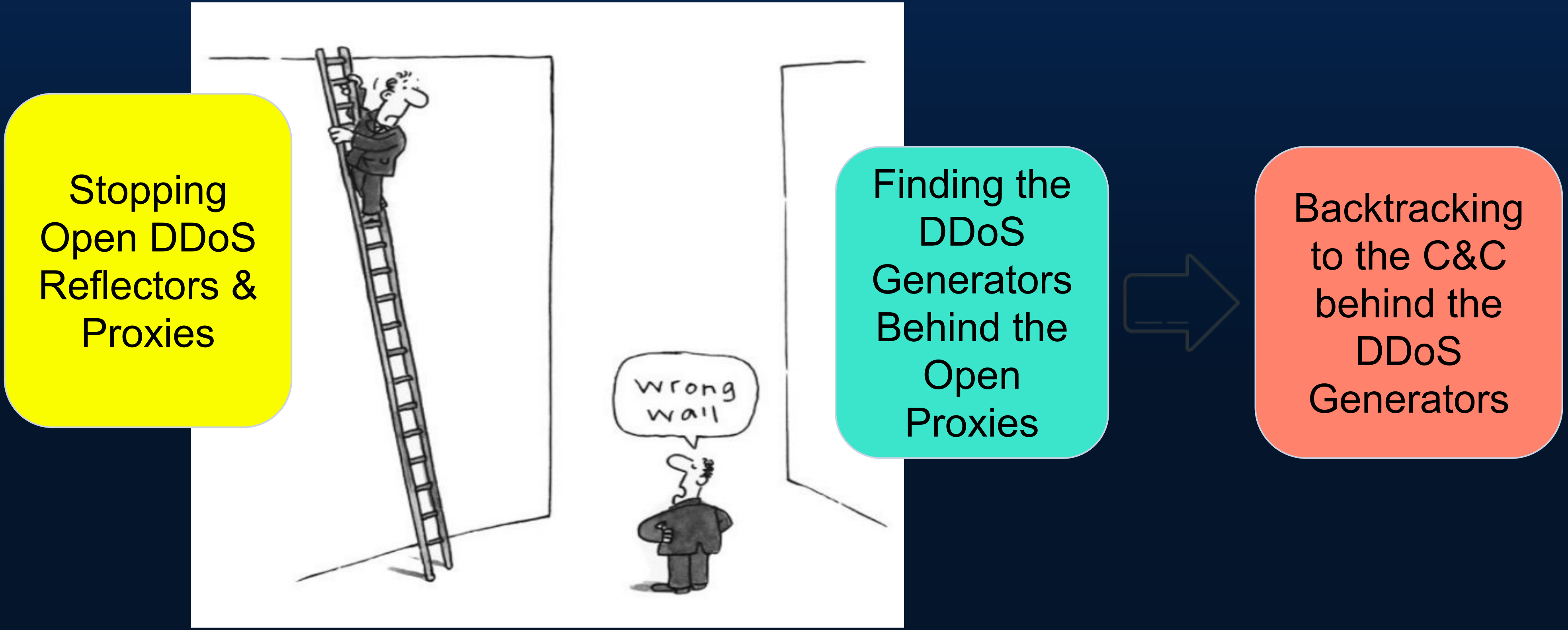
Insanity: doing the same thing over and over again and expecting different results.

Albert Einstein

German Theoretical-Physicist

(1879-1955)

Don't try to fix everything!



Stopping Open DDoS Reflectors & Proxies

Finding the DDoS Generators Behind the Open Proxies

Backtracking to the C&C behind the DDoS Generators

Work on the Right Security Problem

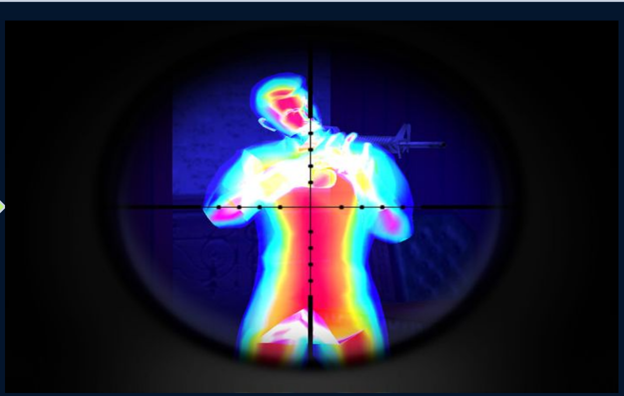
The Good Guys are the Big Part of the Security Problem! Geek out on the “miscreant widgets” forgetting there are always people behind every attack.

This is Nice to Know

The AK-47 was used to rob the bank is = to the phishing was used to get into the bank.

Security Industry Today

Who we need to Target



The people who robbed the bank were tracked via the forensic evidence with a trail that lead to arrest.

Why skull & cross bones? It is only a matter of time before miscreant mischief will lead to death as a factor of “collateral damage”

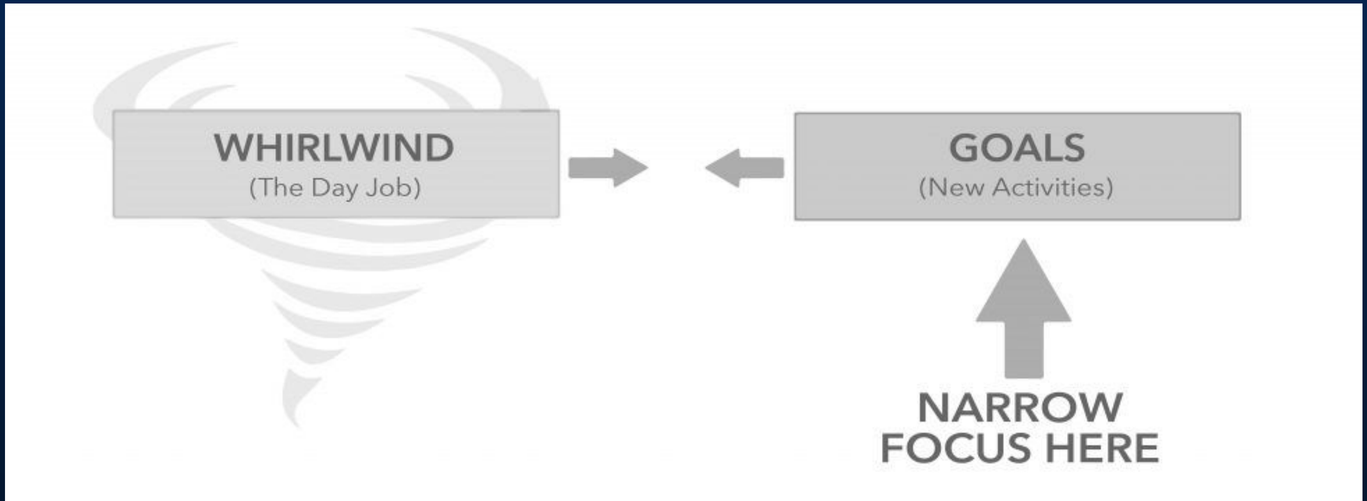
Moneyball the Movie - Inspiration of Rethinking

Moneyball: The Art of Winning an Unfair Game is a book by Michael Lewis, published in 2003, about the Oakland Athletics baseball team and its general manager Billy Beane. Its focus is the team's analytical, evidence-based, sabermetric approach to assembling a competitive baseball team despite Oakland's small budget.

How do you win an unfair game? Rethink the objectives and action!

In Moneyball, the A’s changed their traditional thinking. Rigorous statistical analysis had demonstrated that on-base percentage and slugging percentage are better indicators of offensive success, and the A's became convinced that these qualities were cheaper to obtain on the open market than more historically valued qualities such as speed and contact. ***These observations often flew in the face of conventional baseball wisdom and the beliefs of many baseball scouts and executives.***

Stuck in the Security Whirlwind



We are stuck in the daily Whirlwind of security activities, not stepping back and narrowly focusing on the leading habits that result in major security objectives.

How can we focus on the ~~.5%~~?

We just need the .1%

Collectively, we have the tools identify spoofed miscreant flows, identify reflection elements in networks, backtrace the spoofed flow to the ASN next hop, and pass information to the ASN peer for them to continue the backtrace.

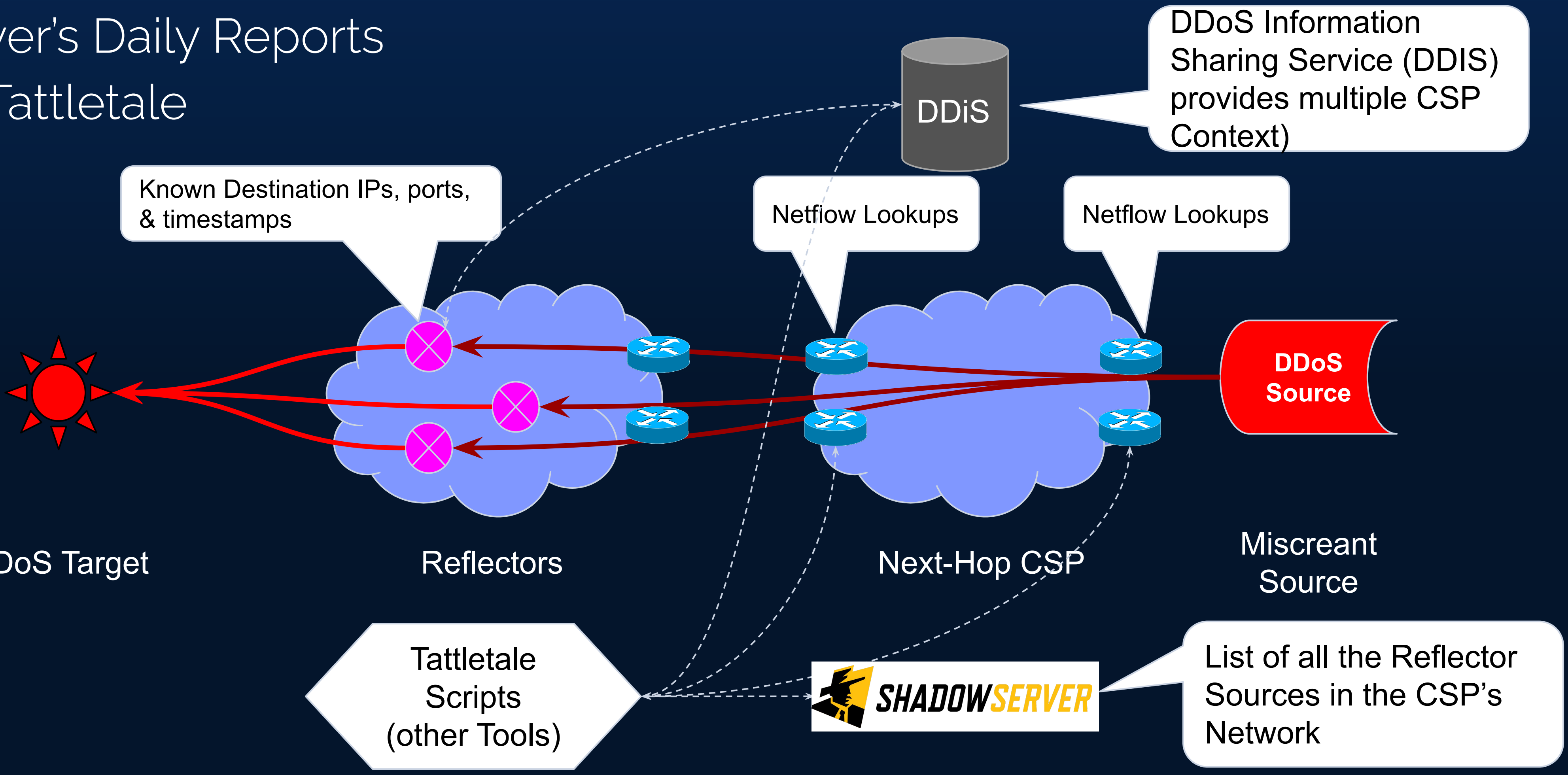
Once identified, DBIT will determine a course of action (applying SAV, working with the network, working with Trust Groups, etc). Over time, the weekly rhythm of backtracking action will identify the problematic .5% “hot spots” on the Internet.

Our Primary Tools

The DDoS Backtracking Toolkit enhance the basics:

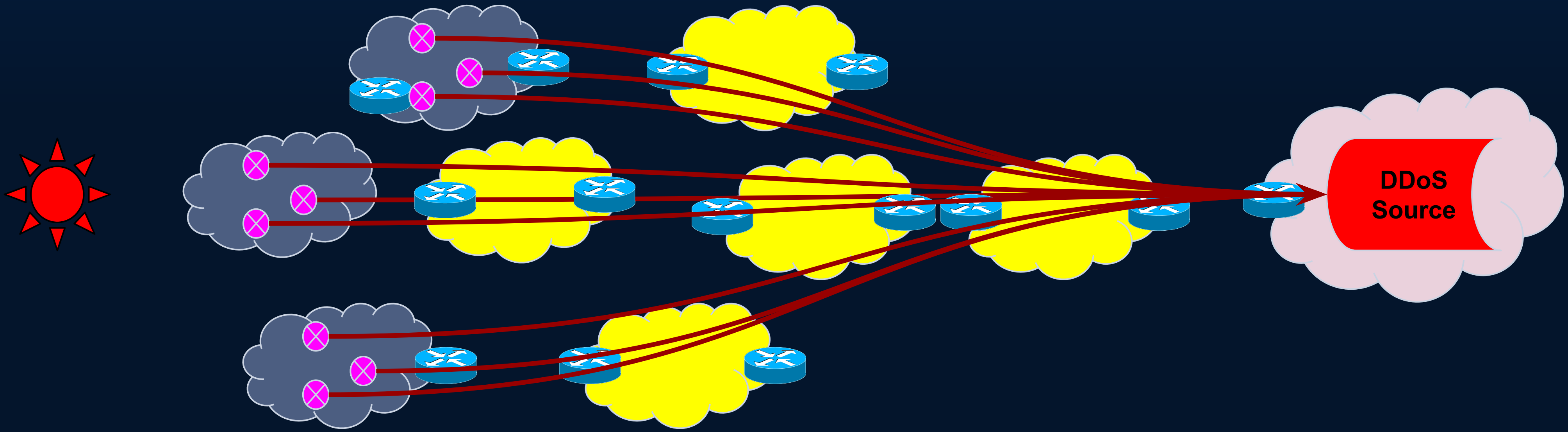
- Netflow
- Shadowserver's Daily Reports
- Scripts like Tattletale

❑ Know all the reflector sources
❑ Know which are used for attack
❑ Know the Netflow data
❑ Know context from DDIS
❑ Know the Upstream ASN


DDiS
DDoS Information Sharing Service (DDIS) provides multiple CSP Context)
Known Destination IPs, ports, & timestamps
Netflow Lookups
Netflow Lookups
DDoS Source
DDoS Target
Reflectors
Next-Hop CSP
Miscreant Source
Tattletale Scripts (other Tools)
SHADOWSERVER
List of all the Reflector Sources in the CSP's Network

DBIT - Tenacious Engagement

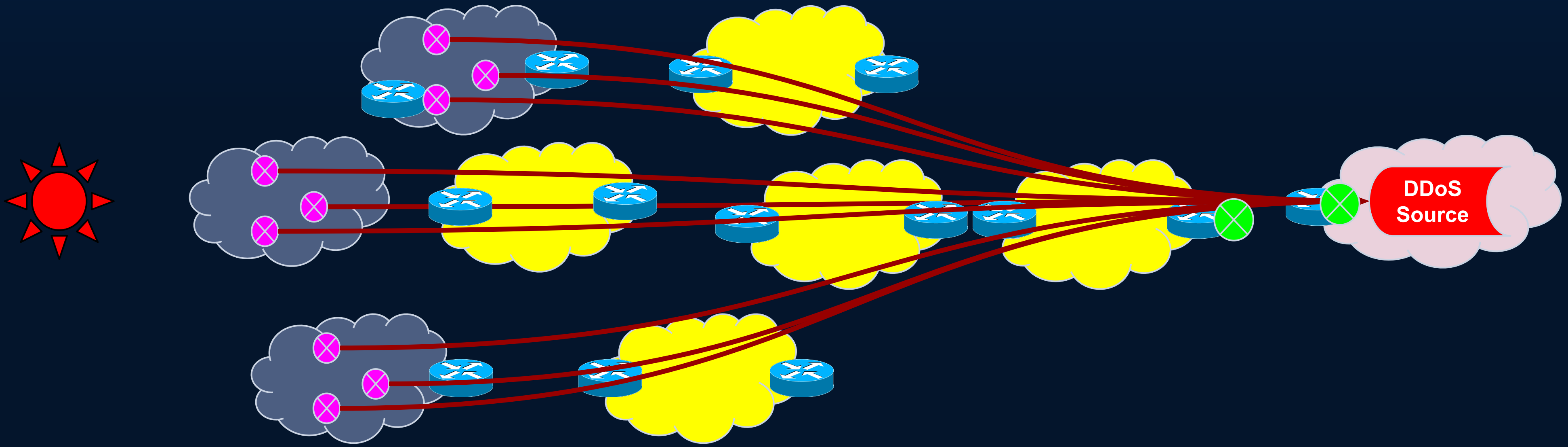
1. Monday List of 3 - 6 protocols with 3 backtrack request.
2. Find the ASN for which the spoof traffic is arriving. Share with the community (via Slack).
3. Tag (using @(name) in Slack or 1:1 DM to move to the next ASNs.
4. Next ASNs find the "next hop ASN" for which the spoofed traffic arrived. Share with the community (via Slack)
5. Continue.



Miscreant Reaction - Instigating Movement

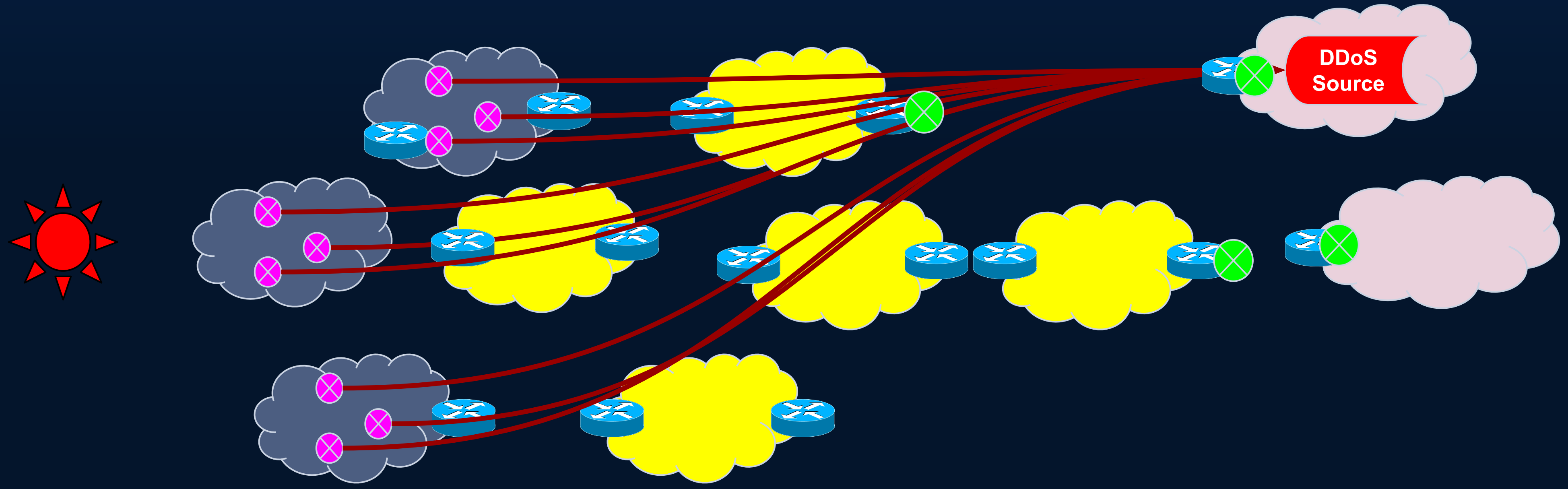
We backtrack to the source, analyze the situation, then take “appropriate action.” We can monitor (sharing the data), apply rate limiting, put ACLs, de-peering, Smoke Jumping, or any other action … as long as we do it weekly.

… For example, apply Source Address Validation (SAV)



Miscreant Reaction - Instigating Movement

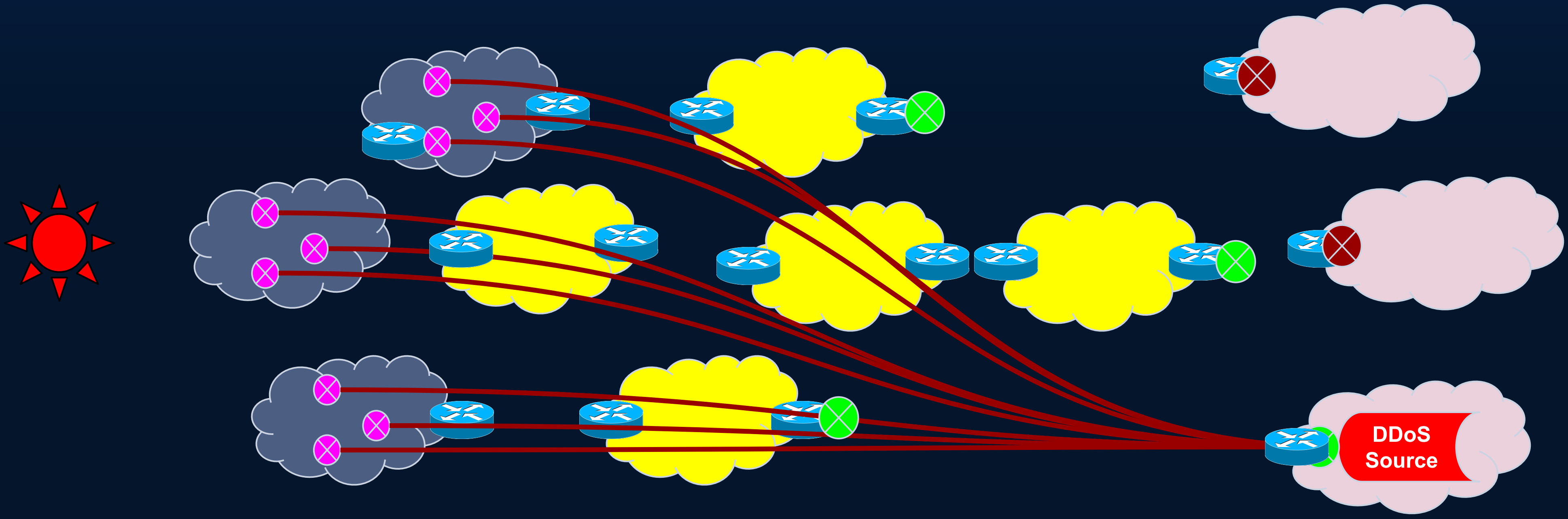
We continue to backtrack each week, analyze the situation, then take “appropriate action.” Applying SAV on the next location.



Miscreant Reaction - Instigating Movement

Over time:

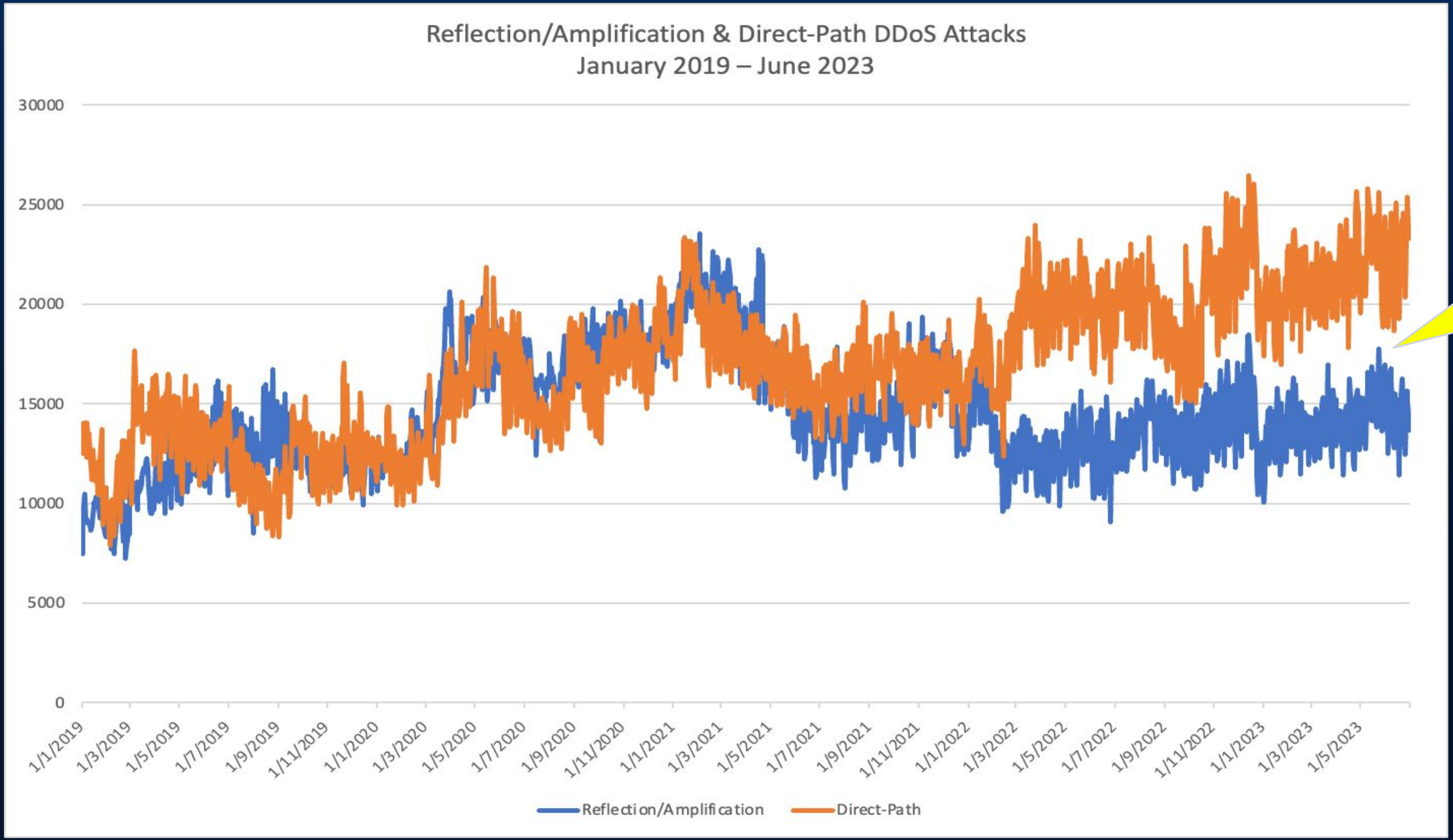
- We plug the holes for each of the locations the DDoS Miscreants host their operation.
- We project cost back on the miscreants - forcing them to change locations.
- Movement focuses miscreants to make mistake (classic military tactic to dislodge a entrenched force).
- We build a community of action pushing back on the miscreants.



The Big Question …

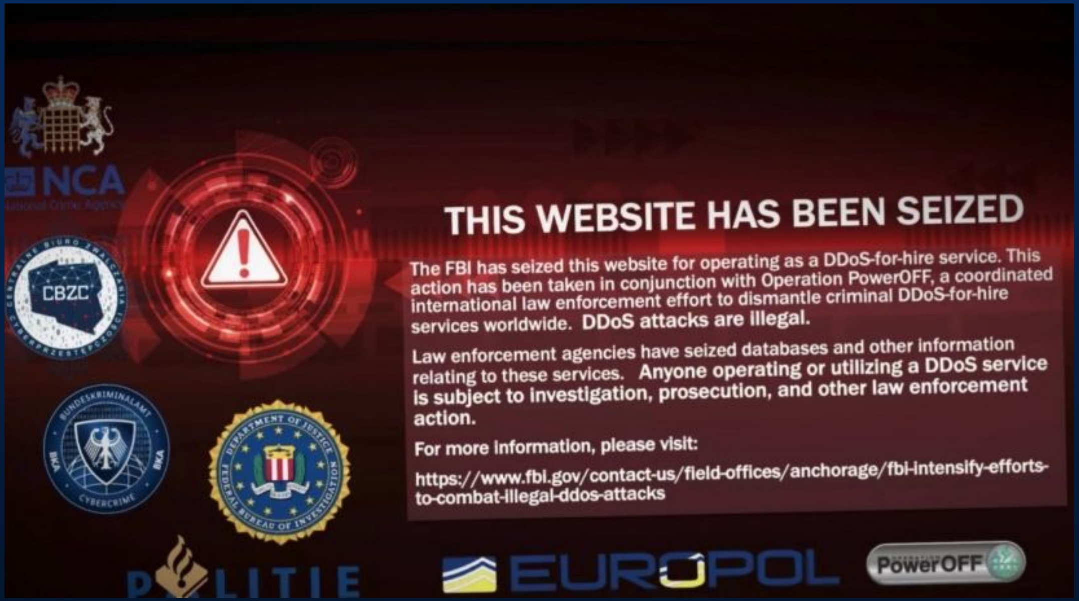
…. is it working?

DDoS Suppression Work!



Using the NetScout DDoS Surface area of DDoS Detection, We see pressure on the DDoS Reflection activities.

We're coming for you .....

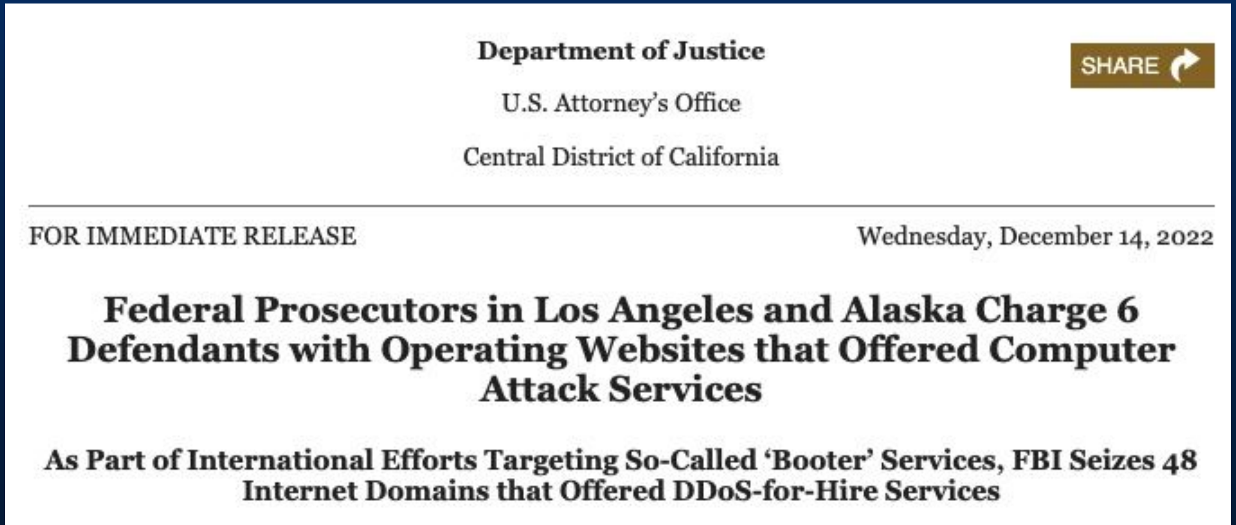


THIS WEBSITE HAS BEEN SEIZED

The FBI has seized this website for operating as a DDoS-for-hire service. This action has been taken in conjunction with Operation PowerOFF, a coordinated international law enforcement effort to dismantle criminal DDoS-for-hire services worldwide. **DDoS attacks are illegal.**

Law enforcement agencies have seized databases and other information relating to these services. **Anyone operating or utilizing a DDoS service is subject to investigation, prosecution, and other law enforcement action.**

For more information, please visit:
https://www.fbi.gov/contact-us/field-offices/anchorage/fbi-intensify-efforts-to-combat-illegal-ddos-attacks



Department of Justice

U.S. Attorney's Office

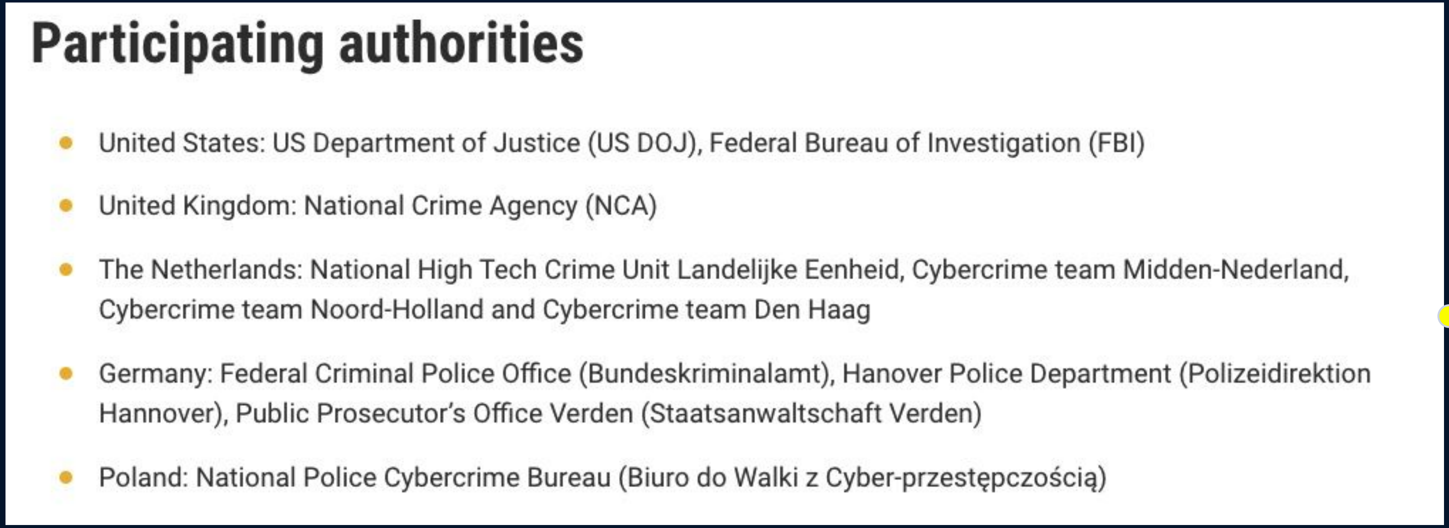
Central District of California

SHARE

FOR IMMEDIATE RELEASE — Wednesday, December 14, 2022

Federal Prosecutors in Los Angeles and Alaska Charge 6 Defendants with Operating Websites that Offered Computer Attack Services

As Part of International Efforts Targeting So-Called 'Booter' Services, FBI Seizes 48 Internet Domains that Offered DDoS-for-Hire Services

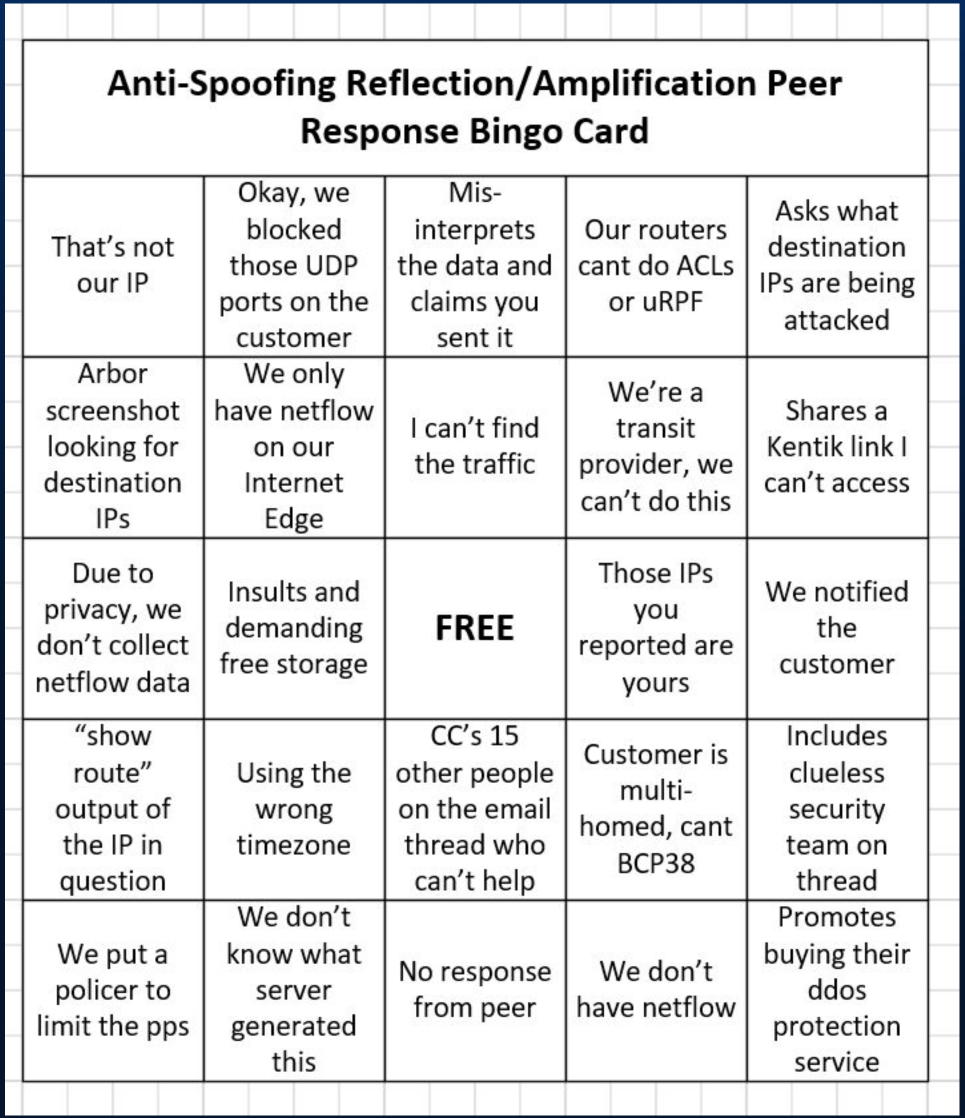


Participating authorities

- United States: US Department of Justice (US DOJ), Federal Bureau of Investigation (FBI)
- United Kingdom: National Crime Agency (NCA)
- The Netherlands: National High Tech Crime Unit Landelijke Eenheid, Cybercrime team Midden-Nederland, Cybercrime team Noord-Holland and Cybercrime team Den Haag
- Germany: Federal Criminal Police Office (Bundeskriminalamt), Hanover Police Department (Polizeidirektion Hannover), Public Prosecutor's Office Verden (Staatsanwaltschaft Verden)
- Poland: National Police Cybercrime Bureau (Biuro do Walki z Cyber-przestępczością)

… and the quiet list of industry & academic institutions who have been pushing back …

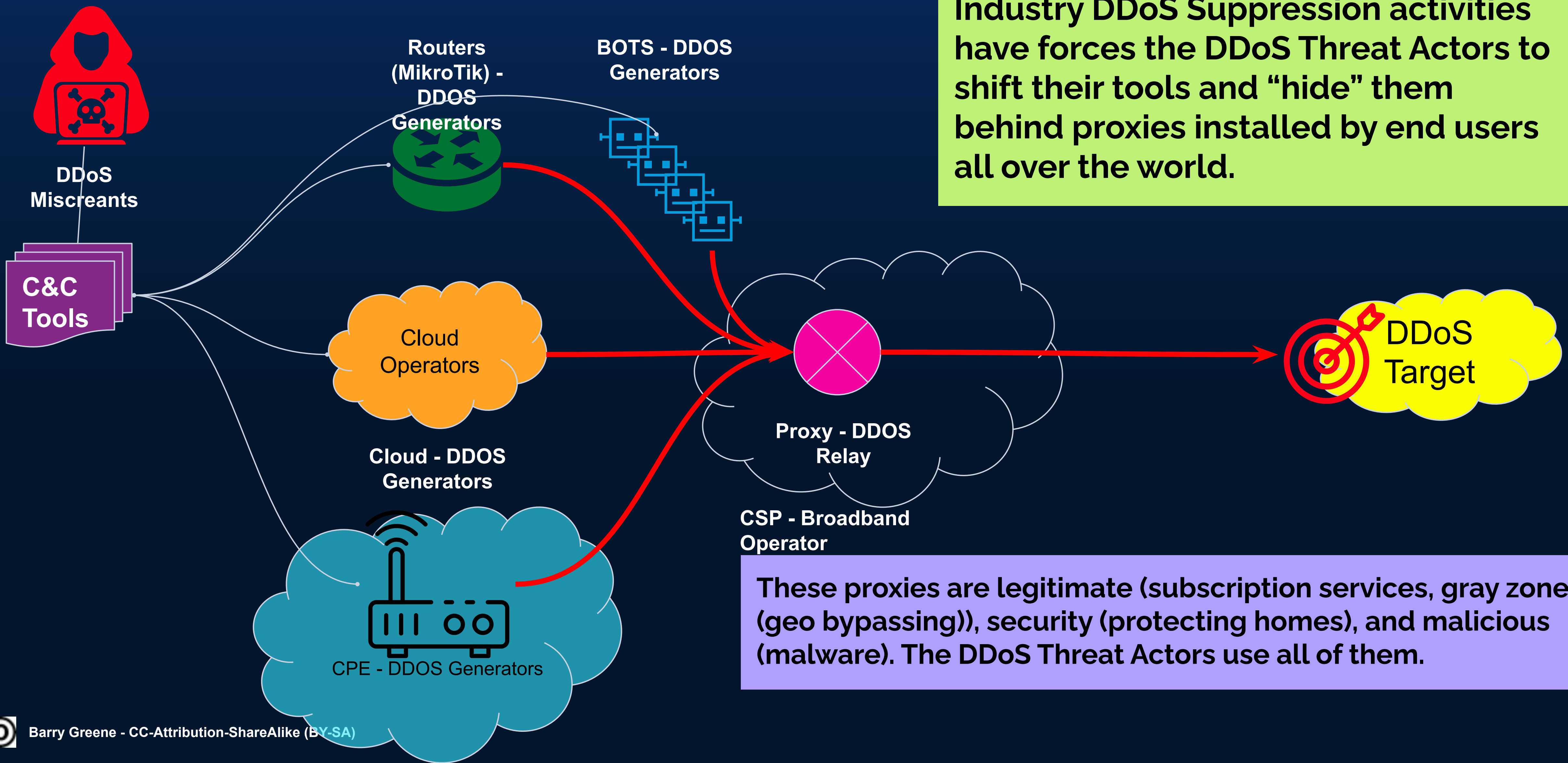
Do we run into problems?



Anti-Spoofing Reflection/Amplification Peer Response Bingo Card

That’s not our IP	Okay, we blocked those UDP ports on the customer	Mis-interprets the data and claims you sent it	Our routers cant do ACLs or uRPF	Asks what destination IPs are being attacked
Arbor screenshot looking for destination IPs	We only have netflow on our Internet Edge	I can’t find the traffic	We’re a transit provider, we can’t do this	Shares a Kentik link I can’t access
Due to privacy, we don’t collect netflow data	Insults and demanding free storage	**FREE**	Those IPs you reported are yours	We notified the customer
“show route” output of the IP in question	Using the wrong timezone	CC’s 15 other people on the email thread who can’t help	Customer is multi-homed, cant BCP38	Includes clueless security team on thread
We put a policer to limit the pps	We don’t know what server generated this	No response from peer	We don’t have netflow	Promotes buying their ddos protection service

Proxies used for DDoS



Industry DDoS Suppression activities have forces the DDoS Threat Actors to shift their tools and “hide” them behind proxies installed by end users all over the world.

These proxies are legitimate (subscription services, gray zone (geo bypassing)), security (protecting homes), and malicious (malware). The DDoS Threat Actors use all of them.

We are seeking wider and ACTIVE Peers

Worried about DDoS? If you are interested in getting special briefings about DBIT, DDIS, Tattletale, or other parts of the collaborative work, reach out to Barry Greene (bgreene@senki.org). He will setup a briefing session with your leadership..

We are seeking:

- More Operators to join the effort who will be active and participate.
- Contributors to open source, community investments into our DDoS Cyber Civil Defence (contributors = volunteer time and funding)