Cyber DIVISION

FEDERAL BUREAU OF INVESTIGATION

NCIS

28 October 2019

Your AS is Mine: BGP/IP Hijacking, the ICBM of the Cyber World

The purpose of this presentation is to:

- Introduce ourselves to the NANOG community
- Share our concerns regarding BGP/IP hijacking
- Request your assistance in identifying, reporting, and working with us to mitigate these issues as they arise

Legend

- Border Gateway Protocol (BGP) – The standard exterior gateway network protocol used to route network traffic between Autonomous Systems (AS) over the Internet.
- Autonomous System – A collection of connected Internet Protocol (IP) routing prefixes (i.e. 11.0.0.0/8) under the control of one or more network operators on behalf of a single administrative entity (i.e. DOD).
- BGP/IP Hijacking – Perpetrator(s) using another entity's IP addresses and/or AS' to send / receive / manipulate network traffic.
- Darkspace – Routable IP addresses where the owner (i.e. USG) does not advertise routes for them over the Internet.

BGP/IP Hijacking Fallacies

- It's Industry Standard Squat Space
  - No such thing…
- IP Squatting/BGP/IP/AS Spoofing Hijacking is not illegal
  - Yes, it is. Theft of Services and Fraud.
- We are not hurting anyone or impacting the owners of the IP space
  - This is a very bad assumption. You don't know what you don't know…
- It's only Internet Noise
  - No such thing… There is always a source and purpose of the traffic emitting through the hijacked IP space.
- If we don't see it, it does not exist
  - This is more related to victims and to put it bluntly is the viewpoint of ignorant and/or arrogant folks. You would be surprised who fits into this category…

BGP/IP Hijacking and AS Spoofing Uses

- Internal Network Address Translation (NAT'ing)
  - This is no problem except when edge routers are misconfigured and leak their routes into the global routing tables.
- Squatters
  - This would include legit companies, Internet Service Provider's (ISP's), or anyone else who advertises BGP routes for IP prefixes they do not own or have permission to use from the owners. This would include RFC 1918 and bogon IP ranges.
  - Question: Why do ISP's route RFC 1918/Bogon prefixes outside of their edge routers?
- Spammers
  - One of the major players in the BGP/IP hijacking area as you know are Spammers. They like to use fraudulently obtained AS', spoof dormant AS' or just hijack AS' to route the hijacked IP space they use to send out their garbage.

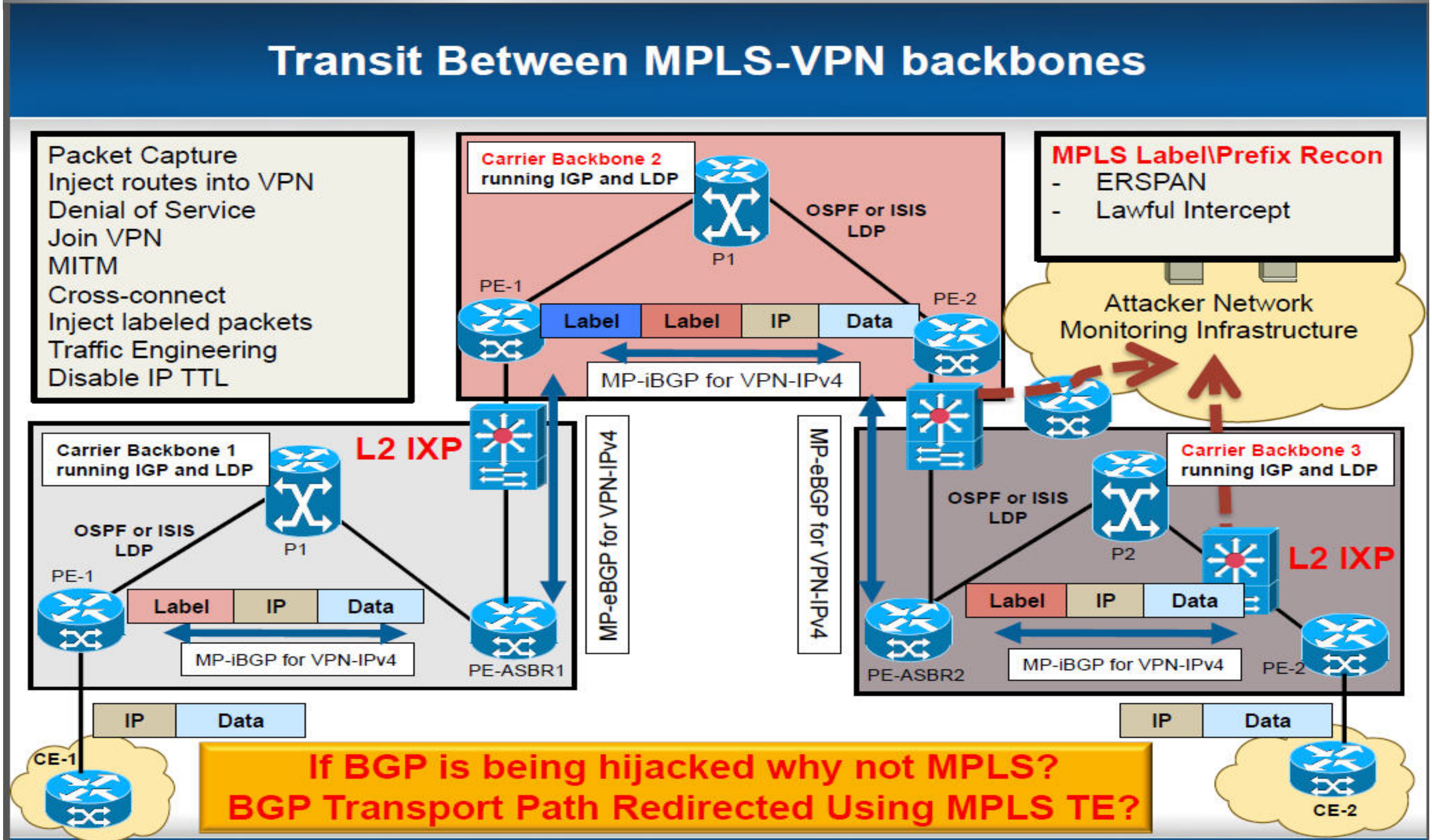
BGP/IP Hijacking and AS Spoofing Uses

- DDoS/BotNet/FastFlux Networks/Dark Web/Malware/Scanning
  - Various types of miscreants on the Internet use BGP/IP hijacking and sometimes couple with AS spoofing to conduct nefarious activities over the Internet. The items listed above are just a small example of what we see occurring within the hijacked IP space.
- Network Intrusions/Command and Control (C2)
  - Miscreants have been seen using both bogon and hijacked IP space as an out of band C2 / data exfil mechanism to facilitate their illicit activities.
- Man-in-the-Middle (MITM) and network traffic redirection
  - Also, we see various types of miscreants conduct BGP MITM attacks to either redirect their victim's network traffic or through some other AS for various purposes or degrade/kill that traffic creating a DoS.

Why Does the USG Care Now?

- The Internet is smaller
  - BGP/IP Hijacking along with AS Spoofing is more noticeable and is actually causing issues with the owners of the hijacked prefixes more and more. Just because a company/org does not advertise global BGP routes for their IP prefixes does not mean they are not being used.
- Used to facilitate illegal activities
  - The majority of the BGP/IP hijacking activity is just the means used to facilitate and obfuscate other malicious and/or illegal activities.
- Loss of money, time and resources
  - The amount of time, money and resources lost when investigating and mitigating BGP/IP hijacking events is becoming more and more expensive.
- Protection of critical infrastructure
  - Common sense or not. We need to protect our national and world critical assets from being affected by this illicit activity that could and has taken down Internet access to entire countries.

What We Are Missing



Transit Between MPLS-VPN backbones

Packet Capture
Inject routes into VPN
Denial of Service
Join VPN
MITM
Cross-connect
Inject labeled packets
Traffic Engineering
Disable IP TTL

MPLS Label\Prefix Recon

- ERSPAN
- Lawful Intercept

If BGP is being hijacked why not MPLS?
BGP Transport Path Redirected Using MPLS TE?

What We Are Missing

- BGP Peering Attacks
  - Sometimes we see BGP peering attacks but a lot of the time we don’t. This is where we need your help in reporting and sharing information about these incidents so we can address them.
- Insider Threats
  - No matter what we are talking about relating to security, the insider threat is the most dangerous and hardest to detect and mitigate. We really need your help in this area. Please share potential/suspected/known insider threat information so we can verify/validate the threat and mitigate it.
- Let us know…
  - We need your input to let us know what we are missing. You are the folks on the ground working routing/backbone Internet issues each day. Help us stay informed so we can help you, your employers, and your customers.

Cyber Initiative and Resource Fusion Unit

- CIRFU
  - FBI HQ Unit collocated at the National Cyber-Forensics and Training Alliance (NCFTA).
  - Focus on shared cyber criminal services and criminal enterprises
  - Initiatives around criminal schemes: BEC, Ransomware, Phishing and Credential Theft
  - Infrastructure takedowns
  - International LE collaboration
- NCFTA
  - Non-profit cyber fusion center with government and private sector partners
  - Offices in Pittsburgh, New York, and Los Angeles
  - Intelligence sharing, case referrals, case enhancements

FBI Cyber Resources

NCIJTF

FBI Led

24 Partner Agencies

National Cyber-Forensics & Training Alliance

Non-profit; shares resources to identify and stop emerging cyber threats

Cyber Behavioral Analysis Center & Cyber Action Team

Provide analytical and technical support to investigations

CyWatch

24/7 Operation

(855) 292-3937

cywatch@ic.fbi.gov

Cyber Task Forces

Located within
56 local field offices

Focused on cyber security threats

Internet Crime Complaint Center

www.ic3.gov

Ways to Help

- Private Industry has a view that government can't match
  - Leverage your visibility to triage suspicious events and focus our efforts.
  - We can't get there with legal process alone.
  - Link suspicious activity to fraud or victimization with articulable losses
    - Time spent investigating ($$$)
    - Wasted traffic ($$$)
- Keep records of LOAs, other relevant documents

Things to Look For

- Suspicious activity en masse by one organization
- Mismatch of Letter of Authority (LOA) to route
- Fraudulent LOAs (this is wire fraud)
- Manipulation or duplication evident by checking multiple routing registries
- IP blocks listed as ‘X’ but showing up as ‘Y’ somewhere else
- Continued use of ISP resources after banning or blocking due to incomplete cleanup

Common Concerns

- We do not further victimize the victim:
  - Mindful of reputational harm (we will not publicly confirm / deny existence of an investigation)
  - Information that may harm a company is not needlessly disclosed
  - No disclosure to regulators
  - No judgement of adequacy of existing defenses
  - Not an opportunity to look for illegal activity
- Authorization to Share
  - Cyber Information Sharing Act (CISA, 2015)

Benefits of Reporting to the FBI

- Network Defense
  - Two-way sharing of network indicators and known TTPs
  - Central sharing hub so that multiple companies seeing the same thing can benefit (this is the NCFTA's mission)
- Dismantle Infrastructure
  - Botnet takedowns, Domain, Network, and server seizures / sinkholing, victim remediation
- Impose costs on cyber actors
  - Arrests & Extraditions / Indictments & Inability to travel
- Recover losses
  - IC3 Recovery Asset Team (75% recovered in 2018)

Recent Example - Micfo

- Amir Golestan - Indicted April 2019 on Wire Fraud charges (fraudulent documents)
- Created 10 “channel” (shell) companies with fictitious representatives and customers as justification for requesting ~750,000 IP addresses from ARIN (worth $10-15M)
- We used IPv4-address secondary markets to determine the value of an IP address
- We relied heavily on information and records provided by ARIN to show the fraud

Conclusion

- Truly, we are the Government and we are here to help
- We do understand and care about BGP/IP Hijacking issues
- With your help, insight, and expertise we will be able to make an impact against the malicious cyber actors who operate in this space

Contact Us

- Tim Fowler
- Task Force Member
- Naval Criminal Investigative Service
- FBI - Cyber Task Force
  Huntsville, AL
- Desk: (256) 213-2760
- Cell: (256) 527-5621
- Email: tfowler@ncis.navy.mil
- PGP Fingerprint:
  - A2A2 6344 1E20 C823
    C9FD 87DB 5957
    FF15 FC2E 88E9

- Chris Elverson
- Supervisory Special Agent
- FBI Cyber Division
- Liaison at NCFTA
  Pittsburgh, PA
- Cell: (313) 670-6824
- Email: cwelverson@fbi.gov
- PGP Fingerprint:
  - 7009 3CF3 96E3 316F
    5B98 DE68 6CF5
    CADE 163E 1996