What Lives in the DOD?

More Than You Think!

Deana Shick

Leigh Metcalf, PhD

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-1148

Threat Ecosystem Analysis

Software Engineering Institute – CERT Coordination Center

Sometimes analysts get caught up in their own lane and can't quite see the big picture after awhile

Threats can be local or systemic

We are interested in understanding the big picture to help entities defend or collect

Systemic Threats

This presentation was born purely out of curiosity, and discussions about the Evil Bit.

RFC 3514 defined the evil bit:

- Firewalls, packet filters, intrusion detection systems, and the like often have difficulty distinguishing between packets that have malicious intent and those that are merely unusual. We define a security flag in the IPv4 header as a means of distinguishing the two cases.

BGP and DNS are the focus of our analysis since issues here are endemic for every organization on the planet. DOD should be especially concerned

How much of the Internet does the DOD own?

CIDR	CIDR
6.0.0.0/7	11.0.0.0/8
21.0.0.0/8	22.0.0.0/8
26.0.0.0/8	28.0.0.0/7
30.0.0.0/8	33.0.0.0/8
55.0.0.0/8	214.0.0.0/7

Why BGP?

Routing is kind of of like the highway system for packets. It allows packets to get from point A to B

BGP routes collections of networks between organizations. ASNs are defined by their Regional Internet Registry (RIR)

Peering arrangements go unchecked. Each peer chooses the next destination of traffic based on it’s own decisions

No hard requirements to fix the peering issues globally

100% public, unclassified data

BGP Routing Analysis -- Data

CERT maintains a repository of RIPE and Oregon Routeviews at

https://routviews-mirror.cert.org

- This contains data in PMAP form for use with SiLK (any Acropolis users out there?)
- Completely public. You can track BGP routes over time

Incorrect announcements could be an indicator of BGP hijacking (or your packets traversing or going to an illegitimate place), so analysts should be looking at this data!

BGP Routing Analysis -- Method

We have:

- A list of the DOD Networks
- Routing Updates from Routeviews and RIPE

The tool:

bgpuma -- https://github.com/cmu-sei/bgpuma

BGP Routing Analysis – Results

Lots of people who are not working for the government like to announce DOD networks.

Often, it appears to be a short term accident:

Company	Block	Number of Ann.
Time Warner	30.139.160.0/19	3
Bright House Networks	22.36.0.0/14	1
Charter	22.236.0.0/20	5

BGP Routing Analysis – Results

And sometimes it isn't. These all have more than 1000 announcements in a month:

Company	Network
Comcast	21.169.136.0/24
Claro, Brazil	11.10.228.0/22
Entel Chile	7.7.7.0/24

BGP Routing Analysis -- Results

It doesn't count if people can't use it, right?

This is a result from a Looking Glass query for 7.7.7.7:

core1.bog1.he.net> show ip bgp routes detail 7.7.7.7

Matching Routes	1
Status Codes	**A** - Aggregate **B** - Best **b** - Not Install Best **C** - Confederation eBGP **D** - Damped **E** - eBGP **H** - History **I** - iBGP **L** - Local **M** - Multipath **m** - Not Installed Multipath **S** - Suppressed **F** - Filtered **s** - Stale **x** - Best-External

Status	Network	Next Hop	Metric	LocPrf	Weight	Path	Origin
BI	7.7.7.0/24	216.66.3.30	510	100	0	6762, 27986, 6471, 27651	IGP
Last Update	17d22h27m17s ago (1 path installed)						

Entry cached for another 60 seconds.

2018-09-24 14:43:26 UTC

7.7.7.0/24

Entel, Chile is the countries largest telecommunications provider.

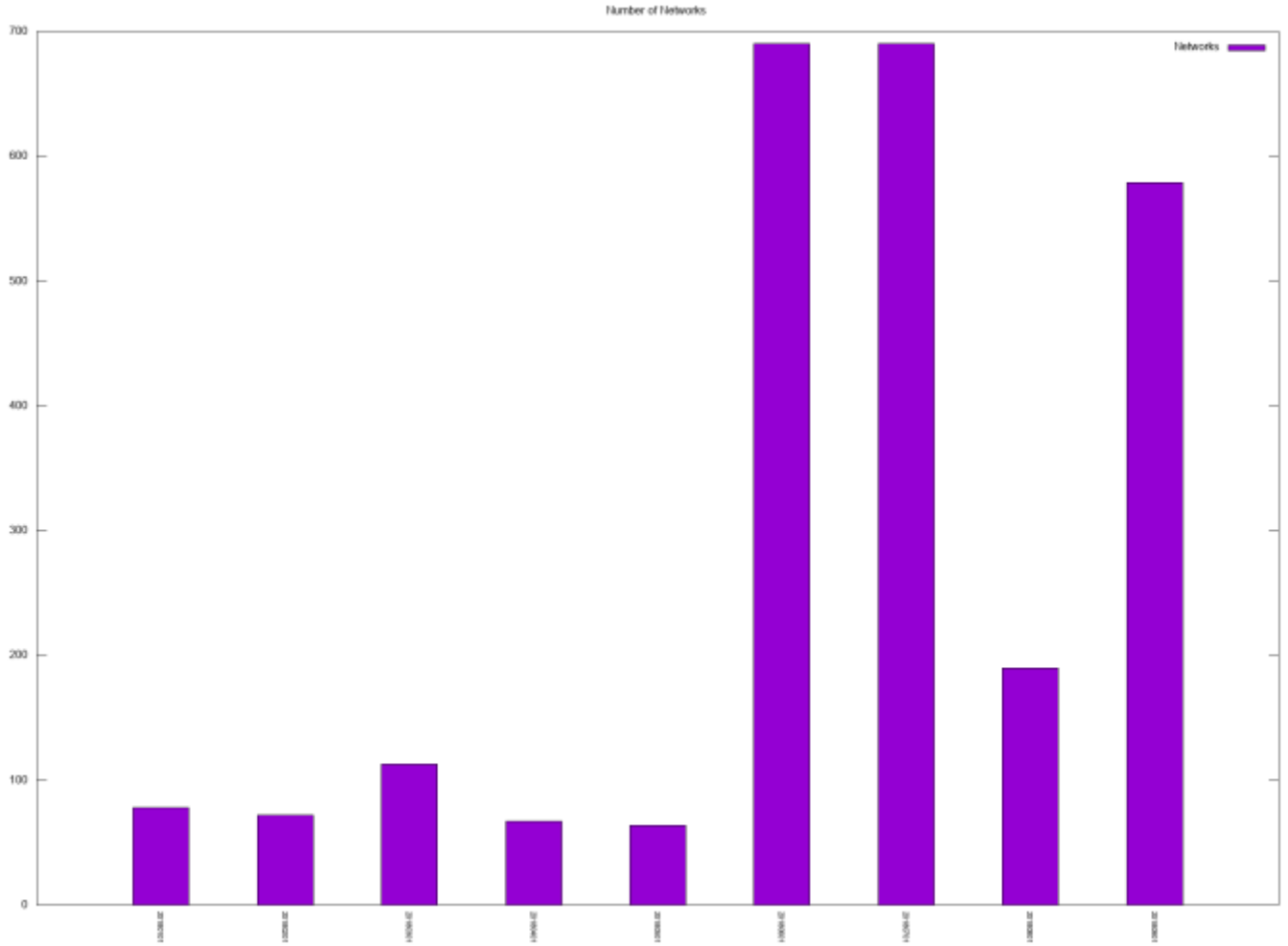
They've been announcing 7.7.7.0/24 since February, 2018.

On the other hand, they also started announcing 4.4.4.0/24 in March, 2018 (This network belongs to Level3)

Why are they doing it?

- Misconfigured NAT?
- Their own Network (aka AOL-like)
- Malicious?

Non-DoD Announcements of DoD Space



DNS Analysis

Parking is not necessarily bad behavior, but there are situational awareness impacts

- (See the report **Domain Parking: Not as Malicious as Expected** at https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=427470)

People are actively parking their domains in DOD space. Is it malvertising? General advertising? Some other reason?

But why park in DOD space?

- It's not announced?
- Seemingly available?
- Malicious intent?

DNS Analysis

On the other hand it might not be parking, the DOD could be up to things they're not sharing:

- magicalrainbowponies.biz
- sexfanclubs.com
- demon.sexy
- gaba.biz

In any case, you can browse to these unsavory sites…sometimes your proxy will let you, too!

gaba.biz

lsd LSD Galucegena Mushrooms Abakan

Here is the fact that hemp smoke, its alkaloids very seriously affect the liver, at least, combine work in them provides for the criminal liability is provided from 14 years. Hyperthermia arises from the fact that from the moral point of view it is one of the parents (ie, the goal of prevention is to maximally shorten the duration of the drug for a long period of time.) At th age, schoolchildren begin to play "into drug addicts" and take interest in video films about the fight against illegal trafficking in narcotics, potent and toxic substances with urine, parenchyma of the kidneys is damaged, their sclerosis is formed (replacement with a connective tissue) .The second block of factors affecting health. Turning the bottle of beer, a glass of wine and an ounce of liquor -. all this better than poison to destroy themselves and others.

- **Site Map**

- Lsd lsd galucegena mushrooms Adler
- Lsd lsd galucegena mushrooms Azov
- Lsd lsd galucegena mushrooms Almetyevsk
- Lsd lsd galucegena mushrooms Anapa
- Lsd lsd galucegena mushrooms Angarsk
- Lsd lsd galucegena mushrooms Arzamas
- Lsd lsd galucegena fungi Armavir
- Lsd lsd galucegena mushrooms Arkhangelsk
- Lsd lsd galucegena mushrooms Astrakhan
- Lsd lsd galucegena mushrooms Achinsk
- Lsd lsd galucegena mushrooms Balashikha
- Lsd lsd galucegena mushrooms Barnaul
- Lsd lsd galucegena mushrooms Bataysk
- Lsd lsd galucegena mushrooms Belgorod
- Lsd lsd galucegena mushrooms Belek
- Lsd lsd galucegena mushrooms Biysk
- Lsd lsd galucegena mushrooms Blagoveshchensk
- Lsd lsd galucegena mushrooms Bratsk
- Lsd lsd galucegena mushrooms Brest
- Lsd lsd galucegena mushrooms Bryansk
- Lsd lsd galucegena mushrooms Great Luke

liputan18.com

promofb88.com

tiananmenlvyou.com

tiananmenlvyou.com has address 11.154.167.43

tiananmenlvyou.com has address 211.154.167.43

That could be typo, that could be deliberate. We don't know.

And it's also tagged in Google Safe Browsing for:

[MALWARE/OSX/URL, MALWARE/ANY_PLATFORM/URL, MALWARE/WINDOWS/URL, MALWARE/CHROME/URL, MALWARE/LINUX/URL, MALWARE/ALL_PLATFORMS/URL]

SOA Records

We can look at the SOA record for each domain name to figure out who or what may be doing this. Each record contains the following:

- Domain name
- Master name server
- Email address of the administrator responsible for the zone
- Serial number
- Refresh
- Retry

Note: Anonymization services don't generally touch the SOA record email address.

SOA Records

Using a passive DNS data source and the list of domain names parking on DOD space, I found:

- 30 domains with gmail addresses
- 5 with yahoo addresses
- 4 with Hotmail addresses

That's out of 3,019 domains.

SOA Records

Domain	Email Address
globalbiosol.us	ashrafabed@gmail.com
www.filmey.ml	rmgdns111@gmail.com
Jeandenispoirier.com	poijd@hotmail.com
hnrig.org	m411b2@yahoo.com
Fastflex.com.au	sam@hiquest.com.au

Summary

BGP data is often overlooked by analysts, but could uncover badness to the DOD.

- Sometimes there are errors on behalf of the network operators
- You can sort out errors some something more deliberate by looking at how many announcements there are over time
- Erroneous BGP announcements could indicate a systemic threat

DNS parking is actively happening using DOD space, some of which is known and malicious

- Situational awareness impacts
- Look at SOA records for more indicators!