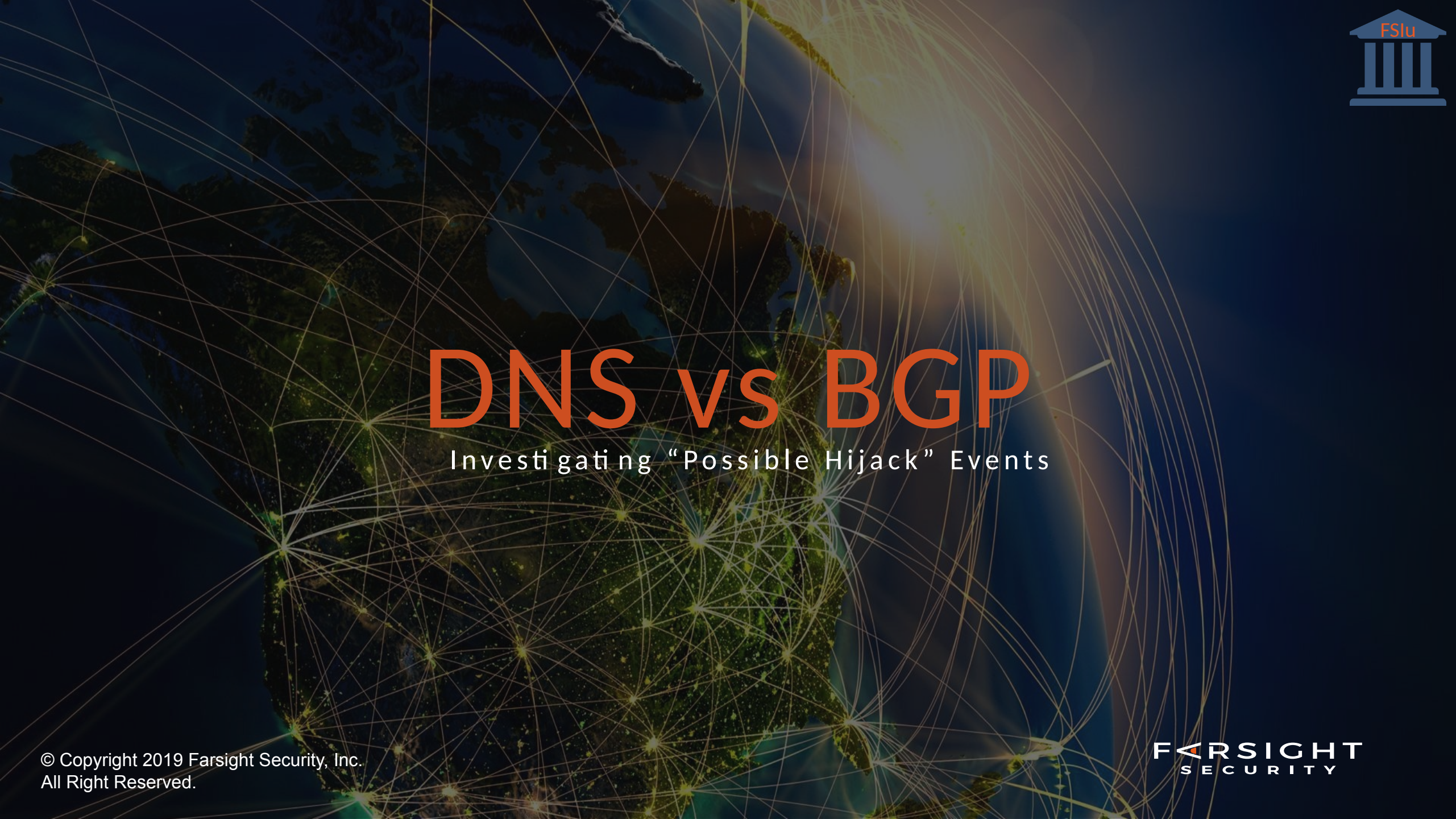


DNS vs BGP

Investigating "Possible Hijack" Events

© Copyright 2019 Farsight Security, Inc.
All Right Reserved.

FARSIGHT SECURITY

PassiveDNS being used for BGP investigation isn't new

Great presentation (I'll use an example from here later)

https://dyn.com/blog/bgp-dns-hijacks-target-payment-systems/

Methodology

Fetch the event list from https://bgpstream.com .

For any row that says “Possible BGP Hijack”, fetch the incident URL.

In the incident report, we’ll see:

```
But beginning at [$DATE], the same prefix
($PREFIX/$MASK) was also announced by ASN $AS.
```

Let’s look at the PassiveDNS history for the network.

One result could be rerouting already-named resources

Another result, what we’re focussing on here, is seeing if someone stands up a nameserver to serve different names during a hijack

Methodology

For each incident:

1. Lookup all NAMEs for which we have A or AAAA records in $ADDRESS/$MASK in recent history (let's say "loosely" 60 days before the start time).

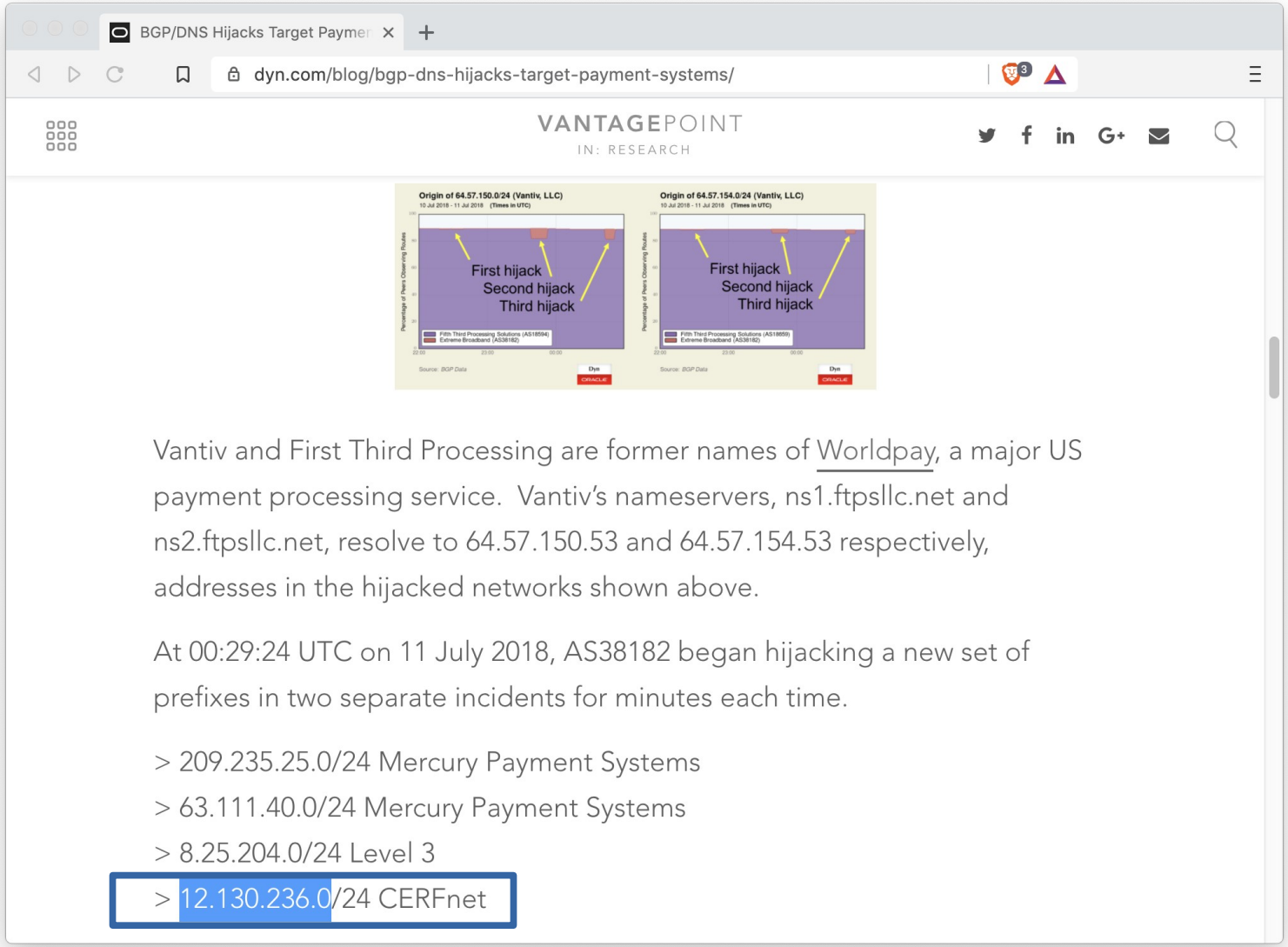
2. For each $NAME,
   Lookup all DOMAIN names that have NS records pointing to the $NAME.

3. For each $DOMAIN,
   Lookup all A or AAAA DNS records in the $DOMAIN that have a short-lived answer. The first_seen time must be >= hijack time and the last_seen time must be less than a day later.

4. Show differences

Back to a known example

Worldpay ns[12].ftpsllc.net 64.57.150.53
==> prod.ssl53.com?



Look at scripting results and PassiveDNS data in terminal windows.

pillkahn

Possible BGP hijack

Beginning at 2019-12-09 20:54:29 UTC, we detected a possible BGP hijack.
Prefix 2404:3d00:40b0::/47, is normally announced by AS3573 ACCENTURE - Accenture LLP, US.

But beginning at 2019-12-09 20:54:29, the same prefix (2404:3d00:40b0::/47) was also announced by ASN 60266.

This was detected by 2 BGPMon peers.

Expected
Start time: 2019-12-09 20:54:29 UTC
Expected prefix: 2404:3d00:40b0::/47
Expected ASN: 3573 (ACCENTURE - Accenture LLP, US)

Event Details
Detected advertisement: 2404:3d00:40b0::/47
Detected Origin ASN 60266 (EMBEDIT-AS, CZ)
Detected AS Path 11071 36213 6939 9498 60266
Detected by number of BGPMon peers: 2

pillkahn

False positive – they meant to change?

```
$ dnsdbq -r pillkahn-hosting.de/AAAA
;; record times: 2019-11-28 00:42:07 .. 2019-11-28 00:42:07
;; count: 2; bailiwick: pillkahn-hosting.de.
pillkahn-hosting.de.  AAAA  2a01:7e0:0:405::187a

;; record times: 2019-12-10 06:57:27 .. 2019-12-10 06:57:27
;; count: 3; bailiwick: pillkahn-hosting.de.
pillkahn-hosting.de.  AAAA  2a03:4000:3e:253::1

$ dig +short pillkahn-hosting.de AAAA
2a03:4000:3e:253::1
```

MD hosting

Possible BGP hijack

Beginning at 2019-12-03 15:05:27 UTC, we detected a possible BGP hijack.
Prefix 80.94.80.0/23, is normally announced by AS49443 SISTEME, MD.

But beginning at 2019-12-03 15:05:27, the same prefix (80.94.80.0/23) was also announced by ASN 64470.

This was detected by 145 BGPMon peers.

Expected
Start time: 2019-12-03 15:05:27 UTC
Expected prefix: 80.94.80.0/23
Expected ASN: 49443 (SISTEME, MD)

Event Details
Detected advertisement: 80.94.80.0/23
Detected Origin ASN 64470 (LUCID, MD)
Detected AS Path 61951 262765 16735 3257 8926 41221 35346 35346 35346 35346 35346 35346 35346 35346 3
Detected by number of BGPMon peers: 145

MD hosting

Another false positive

```
$ dnsdbq  -A 2019-11-01 -r writingpurposes.com/A
;; record times: 2019-12-05 05:55:21 .. 2019-12-05 05:55:21
;; count: 2; bailiwick: writingpurposes.com.
writingpurposes.com.  A  80.94.80.194

;; record times: 2019-01-20 15:27:37 .. 2019-11-14 17:56:33
;; count: 174; bailiwick: writingpurposes.com.
writingpurposes.com.  A  192.64.119.40

$ dnsdbq  -A 2019-11-01 -r walkmemories.com/A
;; record times: 2019-12-04 14:24:33 .. 2019-12-04 14:24:33
;; count: 3; bailiwick: walkmemories.com.
walkmemories.com.  A  80.94.80.66

;; record times: 2019-02-22 10:04:18 .. 2019-11-14 17:45:04
;; count: 94; bailiwick: walkmemories.com.
walkmemories.com.  A  192.64.119.133

$ dig +short writingpurposes.com A
80.94.80.194
$ dig +short walkmemories.com A
80.94.80.66
```

NREL

FARSIGHT SECURITY

Possible BGP hijack

Beginning at 2019-12-03 12:32:10, we detected a possible BGP hijack.
Prefix 192.174.32.0/19, Normally announced by AS16411 NREL-AS-NATIONAL-RENEWABLE-ENERGY-LABORATORY - National Renewable Energy Laboratory, US

Starting at 2019-12-03 12:32:10, a more specific route (192.174.58.0/24) was announced by ASN 12552.

This was detected by 9 BGPMon peers.

Expected
Start time: 2019-12-03 12:32:10 UTC
Expected prefix: 192.174.32.0/19
Expected ASN: 16411 (NREL-AS-NATIONAL-RENEWABLE-ENERGY-LABORATORY - National Renewable Energy Laboratory, US)

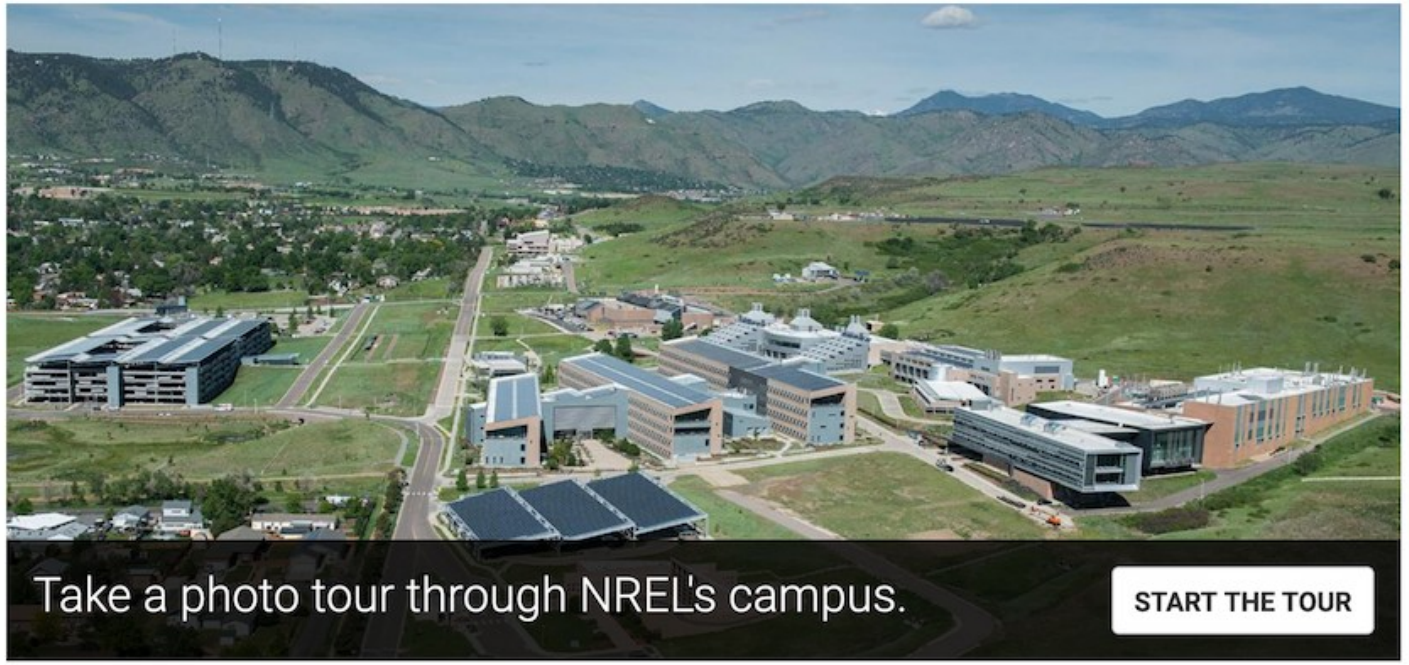
Event Details
Detected advertisement: 192.174.58.0/24
Detected Origin ASN 12552 (IPO-EU, SE)
Detected AS Path 49605 9002 12552
Detected by number of BGPMon peers: 9

NREL

Yes, hijacked IP, but no DNS changes seen
(many nrel.gov, smartgrid.gov, etc.)

About NREL

At the National Renewable Energy Laboratory (NREL), we focus on creative answers to today's energy challenges. From breakthroughs in fundamental science to new clean technologies to integrated energy systems that power our lives, NREL researchers are transforming the way the nation and the world use energy.



IR hosting

Possible BGP hijack

Beginning at 2019-10-27 21:29:41 UTC, we detected a possible BGP hijack.
Prefix 89.32.250.0/24, is normally announced by AS204213 NETMIHAN, IR.

But beginning at 2019-10-27 21:29:41, the same prefix (89.32.250.0/24) was also announced by ASN 43289.

This was detected by 150 BGPMon peers.

Expected
Start time: 2019-10-27 21:29:41 UTC
Expected prefix: 89.32.250.0/24
Expected ASN: 204213 (NETMIHAN, IR)

Event Details
Detected advertisement: 89.32.250.0/24
Detected Origin ASN 43289 (TRABIA, MD)
Detected AS Path 268232 17222 6762 3223 43289
Detected by number of BGPMon peers: 150

IR network migration?

Several Iranian names hosted in the space changed IPs

Eg: warcraft-key.com.

```
;; record times: 2019-06-05 15:53:04 .. 2019-07-01 22:51:32
;; count: 14; bailiwick: warcraft-key.com.
warcraft-key.com.  A  89.32.251.13

--- event was 10/27/2019 ---

;; record times: 2019-10-29 09:49:51 .. 2019-10-29 09:49:51
;; count: 1; bailiwick: warcraft-key.com.
warcraft-key.com.  A  207.244.67.138

--- later disappeared.
```

Consider Iranian network shutdown in November vs hosting in Iran.

During hijack period, yes, several names with A records in 89.32.251.0 could have been monitored or served with a different page.

Failure leads to improving the process

Nothing newsworthy was seen from latest “Possible Hijacks” in last 3 months

PassiveDNS only might miss observation if not a popular name
- Need to do active lookups close to time of outage
- Should repeat every few minutes for a couple hours.

Our sensor poperators might not see the route change
- Need to do lookups from distributed hosting companies.
- “Looker Upper” botnet

DNSDB replaces IP response address with bailiwick
- Need to dump pre-bailiwick stream for changed IPs -- > Names

Timing changes in raw PassiveDNS data
- Could check DNS Observatory for related IPTTL on IP range
- Could create 3-hour watch for raw data in DNS based on IP range

Enhance with other distributed scanning or measurements
- traceroute from multiple places, web scrape, nmap sweep

Data in the DNS stream that could help detect BGP changes

FARSIGHT SECURITY

```
[259] [2019-10-18 12:26:29.673455000]
type: UDP_QUERY_RESPONSE
query_ip: 123.45.67.89
response_ip: 173.245.58.182
proto: UDP (17)
query_port: 3532
response_port: 53
id: 11550
qname: www.legalrc1.com.
qclass: IN (1)
qtype: A (1)
rcode: NOERROR (0)
delay: 0.004214
udp_checksum: CORRECT
```

```
query: [45 octets] (from actual UDP packet)
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 11550
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;www.legalrc1.com. IN A
;; ANSWER SECTION:
;; AUTHORITY SECTION:
;; ADDITIONAL SECTION:
---

response: [77 octets] (from actual UDP packet)
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 11550
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;www.legalrc1.com. IN A
;; ANSWER SECTION:
www.legalrc1.com. 300 IN A 104.27.184.171
www.legalrc1.com. 300 IN A 104.27.185.171
;; AUTHORITY SECTION:
;; ADDITIONAL SECTION:
---
```

DNS Observatory

- **resp_delays**: the quartiles of DNS response delays
  - each value gives 3 numbers (Q1 = 25% percentile, Q2 = median, 50% percentile, Q3 = 75% percentile)
  - the values are separated with the pipe character '|', e.g. "4.47|7.01|8.01" means q1=4.47, q2=7.01, q3=
- **network_hops**: as above, but number of network hops (routers) between the resolver and the authoritative DNS
  - inferred using TTL of IP packets by difference to the closest power of 2 (e.g., 64 - 58 = 6 hops)