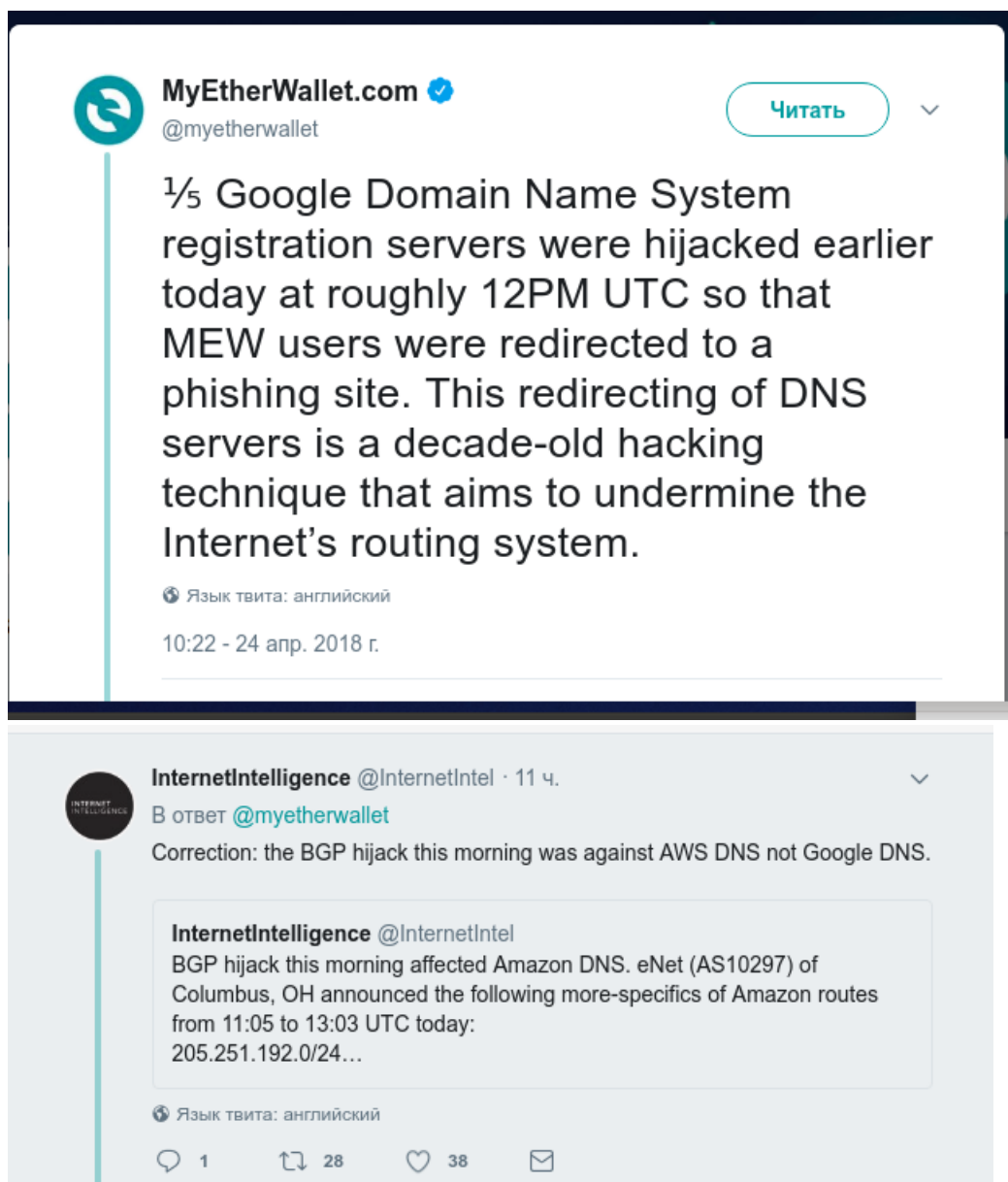


История одного BGP hijack, или необходимо ли фильтровать full-view от аплинков

Идея написать статью о необходимости ревизии принимаемых от аплинков BGP full-view (FV) анонсов возникла еще в конце прошлого года, после обнаруженного большого количества hidden (rejected by import policy) маршрутов принятых после включения очередного аплинка в Казахстане. Более детальный анализ показал "богатость" as-path отфильтрованных по prefix length маршрутов, т. е. специфичных по длине маски чем /24. В тоже время были проанализированы еще с десяток FV от разных апстримов, а также маршруты, принимаемые с обменников (IX - Internet Exchange). По сути оказалось, что дела у остальных обстоят не намного лучше увиденного в Казахстане.

Новые проекты, решение текущих задач отодвинули эту идею на второй план, и в некоторой степени она даже подзабылась. Но произошедший вчера, 24 апреля 2018 года, случай BGP hijack с инфраструктурным значимым префиксом Amazon (для фишинговой атаки на "MyEtherWalet" (MEW)) AS10297 был "угнан" префикс принадлежащий Amazon префикс 205.251.192.0/24, к которому привязаны корневые DNS сервера Amazon. В результате DNS-запросы пользователей, которые в качестве DNS-серверов использовали DNS Amazon перенаправлялись на подменный DNS-сервер злоумышленников, где myetherwallet.com резолвился в IP-адрес фишингового сайта, работающего по протоколу HTTP, т. е. без SSL, или использующего поддельные сертификаты. По сообщениям пользователей Твитер атака длилась несколько часов и злоумышленникам удалось похитить значимое количество криптовалюты благодаря скомпрометированным данным пользователей. Сначала в Твитере [появилось сообщение](#), что это произошло с DNS Google и выглядело очень правдоподобным на фоне наблюдаемых вчера проблем со знаменитыми 8.8.8.8 и 8.8.4.4.



MyEtherWallet.com @myetherwallet

Читать

1/5 Google Domain Name System registration servers were hijacked earlier today at roughly 12PM UTC so that MEW users were redirected to a phishing site. This redirecting of DNS servers is a decade-old hacking technique that aims to undermine the Internet's routing system.

Язык твита: английский

10:22 - 24 апр. 2018 г.

InternetIntelligence @InternetIntel · 11 ч.

В ответ @myetherwallet

Correction: the BGP hijack this morning was against AWS DNS not Google DNS.

InternetIntelligence @InternetIntel

BGP hijack this morning affected Amazon DNS. eNet (AS10297) of Columbus, OH announced the following more-specifics of Amazon routes from 11:05 to 13:03 UTC today: 205.251.192.0/24...

Язык твита: английский

1 28 38

Немного позже пользователи начали оставлять комментарии, что произошедшее случилось все-таки с DNS Amazon.

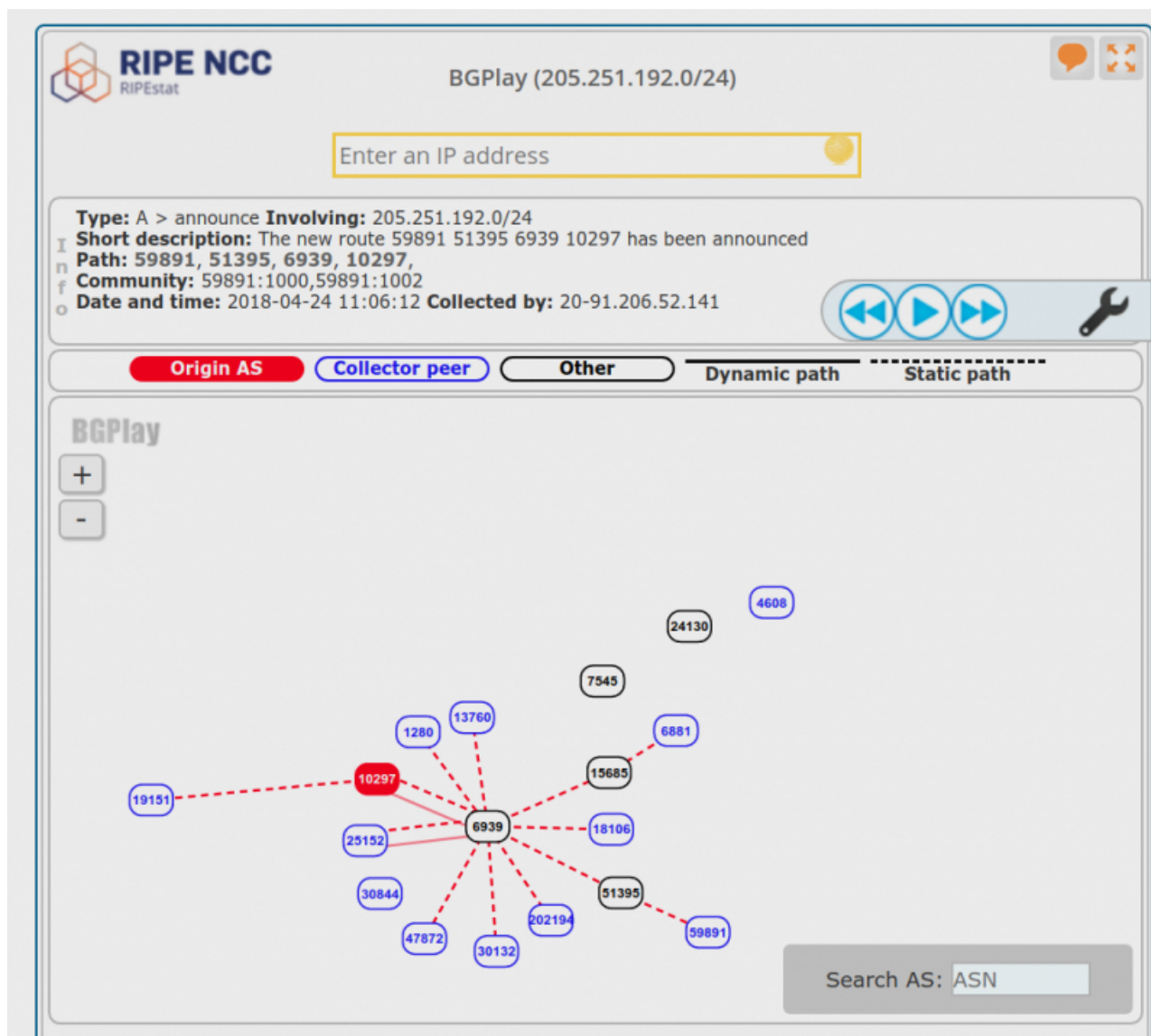
Оригинальный префикс Amazon имеет длину маски /23:

```
whois -h whois.radb.net 205.251.192.0/23 | grep descr
descr:    Amazon prefix
```

```
205.251.192.0/23  *[BGP/170] 2w3d 03:59:28, MED 20, localpref 100
AS path: 3257 16509 I, validation-state: unverified
```

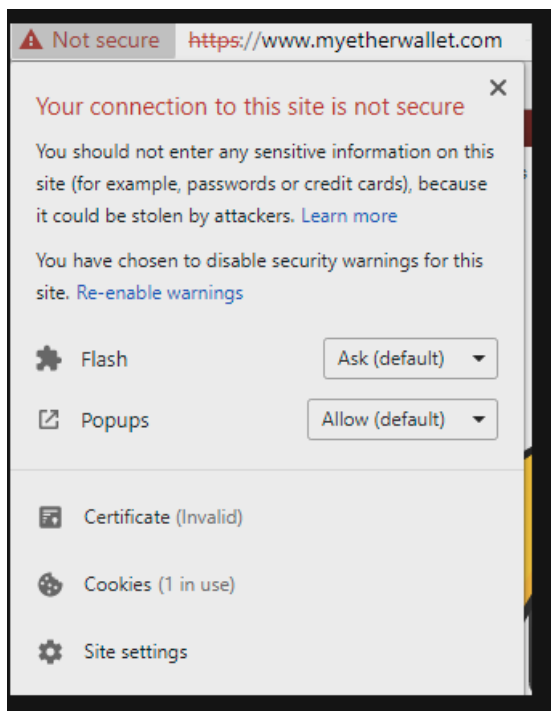
Для атаки был применен так называемый more specific prefix 205.251.192.0/24, который при маршрутизации трафика всегда выигрывает перед less specific 205.251.192.0/23. Данный вид атаки по сути является очень древним, происходит с довольно часто (раз в несколько месяцев случаются довольно громкие события, по значимости аналогичны вчерашнему), и называется BGP Hijack.

Ниже на скриншоте наглядно отображен результат произошедшего с применением аналитического сервиса RIPE BGPlay:



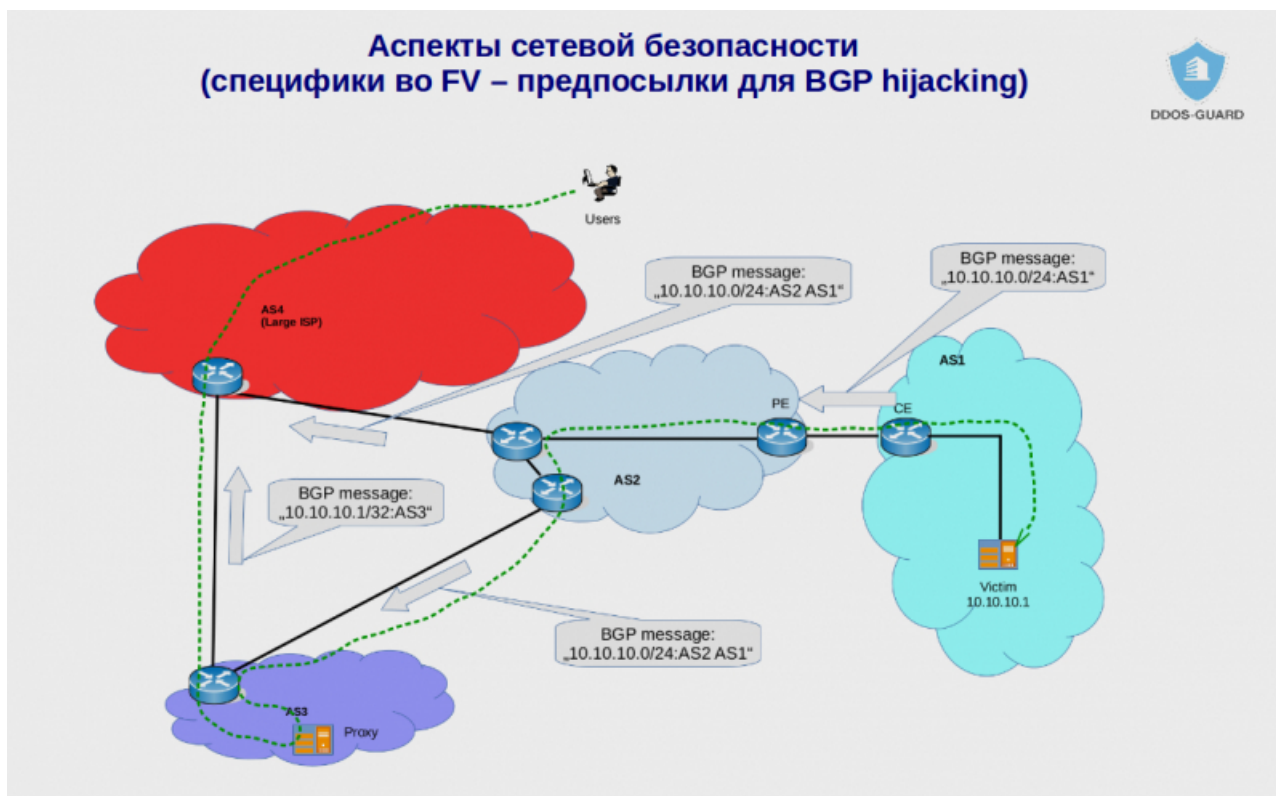
Из данного слайда видно, что префикс был проансирован AS10297 ([eNET Inc.](#), одним из американских хостинг провайдеров) в Tier1 AS6939 (Hurricane Electric), что позволило подвергнуть атаке довольно большое количество автономных систем.

Скриншот браузера при попытке открытия фишингового сайта:



К сожалению, многие пренебрегли подобными предупреждениями.

Из начала статьи можно предположить почему подобное возможно. Ниже представлен слайд презентации из выступления на одном из недавних мероприятий в городе Алма-Ата, наглядно отображающий суть BGP Hijack и не требующий комментариев.



Подобное возможно по двум причинам:

1. Аплинки не осуществляют фильтрацию клиентских анонсов по атрибуту origin с использованием записей из баз IRR (часто причиной тому являются "раздутые" клиентские as-sets и вендорские аппаратные ограничения по количеству строк конфигурационных файлов, но в большей степени - это безразличие, нежелание что-либо внедрять, отсутствие компетенции);
2. Со стороны клиентов нет ревизии принимаемых маршрутов FV на предмет фильтрации не принятых к распространению маршрутов, в т.ч. специфичных чем /24.

```

bravoli# run show route receive-protocol bgp 5.188. table inet.0 hidden
Dec 28 10:58:41
inet.0: 685135 destinations, 685194 routes (680705 active, 0 holddown, 4430 hidden)
Prefix      Nexthop      MED      Lclpref      AS path
1.209.11.240/28 5.188. 59583 62062 60299 31500 3267 2603 4766 38668 I
1.236.0.64/28 5.188. 59583 62062 60299 31500 3267 2603 4766 38396 ?
1.236.2.64/28 5.188. 59583 62062 60299 31500 3267 2603 4766 38390 ?
1.237.2.0/27 5.188. 59583 62062 60299 31500 3267 2603 4766 38392 ?
1.237.2.192/29 5.188. 59583 62062 60299 31500 3267 2603 4766 38392 ?
1.237.4.0/25 5.188. 59583 62062 20764 20764 20764 20764 20764 8732 4766 38395 I
1.238.6.64/28 5.188. 59583 62062 60299 31500 3267 2603 4766 38402 ?
1.238.6.192/29 5.188. 59583 62062 60299 31500 3267 2603 4766 38402 ?
1.238.8.64/28 5.188. 59583 62062 60299 31500 3267 2603 4766 38400 ?
1.238.8.192/29 5.188. 59583 62062 60299 31500 3267 2603 4766 38400 ?
1.238.14.0/28 5.188. 59583 62062 60299 31500 3267 2603 4766 38401 ?
1.238.14.192/29 5.188. 59583 62062 60299 31500 3267 2603 4766 38401 ?
1.238.16.64/28 5.188. 59583 62062 60299 31500 3267 2603 4766 38394 ?
1.238.16.192/29 5.188. 59583 62062 60299 31500 3267 2603 4766 38394 ?
1.238.20.0/27 5.188. 59583 62062 60299 31500 3267 2603 4766 38399 ?
1.238.20.192/29 5.188. 59583 62062 60299 31500 3267 2603 4766 38399 ?
1.238.28.0/25 5.188. 59583 62062 20764 20764 20764 20764 20764 8732 4766 38411 I
1.238.28.128/25 5.188. 59583 62062 20764 20764 20764 20764 20764 8732 4766 38406 I
1.241.0.64/28 5.188. 59583 62062 60299 31500 3267 2603 4766 38408 ?
1.241.2.0/27 5.188. 59583 62062 60299 31500 3267 2603 4766 38403 ?
1.241.2.192/29 5.188. 59583 62062 60299 31500 3267 2603 4766 38403 ?
1.242.4.64/28 5.188. 59583 62062 60299 31500 3267 2603 4766 38407 ?
1.242.6.0/27 5.188. 59583 62062 60299 31500 3267 2603 4766 38414 ?
1.242.6.192/29 5.188. 59583 62062 60299 31500 3267 2603 4766 38414 ?

```

```

bravo9# run show route receive-protocol bgp 5.188.245. table inet.0 hidden
inet.0: 675844 destinations, 2050825 routes (671834 active, 0 holddown, 5489 hidden)
Prefix      Nexthop      MED      Lclpref      AS path
1.209.11.240/28 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38668 I
1.236.0.64/28 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38396 I
1.236.2.64/28 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38390 I
1.237.2.0/27 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38392 I
1.237.2.192/29 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38392 I
1.237.4.0/25 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38395 I
1.238.6.64/28 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38402 I
1.238.6.192/29 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38402 I
1.238.8.64/28 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38400 I
1.238.8.192/29 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38400 I
1.238.14.0/28 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38401 I
1.238.14.192/29 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38401 I
1.238.16.64/28 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38394 I
1.238.16.192/29 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38394 I
1.238.20.0/27 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38399 I
1.238.20.192/29 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38399 I
1.238.28.0/25 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38411 I
1.238.28.128/25 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38406 I
1.241.0.64/28 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38408 I
1.241.2.0/27 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38403 I
1.241.2.192/29 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38403 I
1.242.4.64/28 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38407 I
1.242.6.0/27 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38414 I
1.242.6.192/29 5.188.245. 59583 62062 60299 31500 3267 2603 4766 38414 I

```

```

edit]
bravoli# run show route receive-protocol bgp 5.188. table inet.0 hidden | count
Dec 28 11:02:33
Count: 4433 lines

edit]
bravoli# run show route receive-protocol bgp 5.188. table inet.0 hidden community ".*:666"
Dec 28 11:04:35

inet.0: 685171 destinations, 685231 routes (680740 active, 0 holddown, 4431 hidden)

edit]

```

```

{master}
bravo9> show route receive-protocol bgp 5.188.245.255 hidden | count
Count: 3046 lines

{master}

```

На слайдах выше показаны отфильтрованные в FV маршруты, специфичней чем /24, а также их количество.

Отсутствие подобной фильтрации в операторских сетях позволяет злоумышленникам без каких-либо проблем сделать inject префикса жертвы.

К сожалению, каких-либо жестких ограничений на анонсы спецификов не существует.

В RFC 7454 "BGP Operations and Security", в частности, отмечается, что RIPE рекомендует не

анонсировать и не принимать в Интернет для IPv4 специфичней чем /24, и для IPv6 специфичней /48.

Рекомендую в качестве import policy для аплинков применить что-то подобное и вы увидите в своих таблицах тоже hidden routes :)

```
>show configuration policy-options policy-statement sanity-check-Upstream
term bogons-reject {
  from policy bogons;
  then reject;
}
term bogons-as-reject {
  from as-path grey-as;
  then reject;
}
term long-prefixes-reject {
  from {
    route-filter 0.0.0.0/0 prefix-length-range /25-/32 reject;
  }
}
then next policy;
```