2018

360企业安全（360威胁情报中心）

BGP安全之殇

演讲人：张玉兵（Eric）

引言

BGPv4安全缺陷是全球互联网现存最大最严重的安全漏洞

深度学习

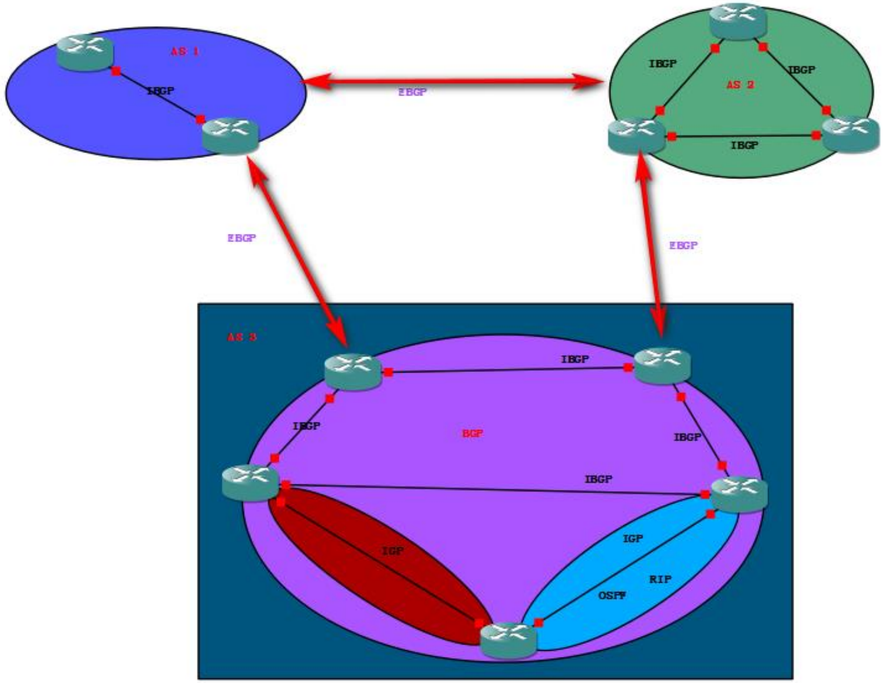
目录
CONTENTS

KCon

PART 01

关于BGP

I’m the BGP protocol.At least so far,nothing is as irreplaceable as me,



BGP（RFC 1771、RFC 4271）：

全称是Border Gateway Protocol, 对应中文是边界网关协议，最新版本是BGPv4。BGP是互联网上一个核心的互联网去中心化自治路由协议。它的地位是核心的毫不夸张地说，**是目前唯一连接海陆空和7大洲4大洋的外部路由协议**。

BGP是最复杂的路由协议，属于应用层协议，其传输层使用TCP，默认端口号是179。因为是应用层协议，可以认为它的连接是可靠的，并且不用考虑底层的工作，例如fragment，确认，重传等等。BGP是唯一使用TCP作为传输层的路由协议，其他的路由协议可能都还到不了传输层。

相关重要概念

AS(Autonomous system):自治系统，指在一个（有时是多个）组织管辖下的所有IP网络和路由器的全体，它们对互联网执行共同的路由策略。也就是说，对于互联网来说，一个AS是一个独立的整体网络。每个AS有自己唯一的编号。通常一个自治系统将会分配一个全局的唯一的16位号码，ASN范围:1-65535;1-64511属于公有ASN，而私有ASN:64512-65535。

AS PATH:路由每通过一个AS范围都会产生一个记录。(路由防环机制)。

EBGP:外部BGP协议(EBGP)的主要作用是向外部路由器或AS提供更多信息。

IBGP:内部BGP协议(IBGP)的主要作用是向AS内部路由器提供更多信息。

BGP的3张表

邻居表(adjancy table):保存所有的BGP邻居信息。
BGP表(forwarding database):保存从每一个邻居学到的路由信息。
路由表(routing table):BGP默认不做负载均衡，会从BGP表中选出一条到达各个目标网络最优的路由，放入路由表保存。路由器只需按路由表保存的路由条目转发数据即可。

邻居表：show ip bgp summary

```
R3_AS30#sh ip bgp summary
BGP router identifier 192.168.50.2, local AS number 30
BGP table version is 17, main routing table version 17
13 network entries using 1521 bytes of memory
32 path entries using 1664 bytes of memory
17/8 BGP path/bestpath attribute entries using 2108 bytes of memory
15 BGP AS-PATH entries using 360 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 5653 total bytes of memory
BGP activity 13/0 prefixes, 34/2 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.30.2     4   200      12      12       17    0    0 00:01:45        6
192.168.30.2    4    20      12      12       17    0    0 00:01:48        8
192.168.40.1    4    40      10      12       17    0    0 00:01:48        8
192.168.50.1    4    50      10      12       17    0    0 00:01:50        6
```

BGP表：show ip bgp

```
R3_AS30#sh ip bgp
BGP table version is 17, local router ID is 192.168.50.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  10.10.220.0/23   192.168.50.1                           0 50 60 100 i
*>                  192.168.40.1                           0 40 100 i
*                   172.16.30.2                            0 200 20 10 100 i
*                   192.168.30.2                           0 20 10 100 i
*  10.10.220.0/22   192.168.30.2                           0 20 200 i
*>                  172.16.30.2              0             0 200 i
*  172.16.30.0/24   172.16.30.2              0             0 200 i
*>                  0.0.0.0                  0         32768 i
*> 172.16.60.0/24   192.168.40.1             0             0 40 i
*                   192.168.50.1                           0 50 60 i
*  172.16.100.0/24  192.168.50.1                           0 50 60 100 i
*>                  192.168.40.1             0             0 40 i
*                   192.168.30.2                           0 20 10 100 i
*  192.168.10.0     192.168.50.1                           0 50 60 100 i
*                   192.168.40.1                           0 40 100 i
*                   172.16.30.2                            0 200 20 10 i
*>                  192.168.30.2                           0 20 10 i
   Network          Next Hop            Metric LocPrf Weight Path
*  192.168.20.0     192.168.40.1                           0 40 100 10 i
*                   172.16.30.2                            0 200 20 i
*>                  192.168.30.2             0             0 20 i
*  192.168.30.0     192.168.30.2             0             0 20 i
*>                  0.0.0.0                  0         32768 i
*  192.168.40.0     192.168.40.1             0             0 40 i
*>                  0.0.0.0                  0         32768 i
*> 192.168.50.0     0.0.0.0                  0         32768 i
*  192.168.60.0     192.168.40.1                           0 40 60 i
*>                  192.168.50.1             0             0 50 i
*  192.168.100.0    192.168.40.1                           0 40 100 i
*                   192.168.30.2                           0 20 10 100 i
*>                  192.168.50.1                           0 50 60 i
*  192.168.200.0    192.168.30.2             0             0 20 i
*>                  172.16.30.2              0             0 200 i
```

路由表：show ip route

```
R3_AS30#sh ip rou
R3_AS30#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.30.0/24 is directly connected, FastEthernet0/1
B    192.168.60.0/24 [20/0] via 192.168.50.1, 00:01:20
B    192.168.10.0/24 [20/0] via 192.168.30.2, 00:01:19
C    192.168.40.0/24 is directly connected, FastEthernet2/0
     172.16.0.0/24 is subnetted, 3 subnets
B       172.16.60.0 [20/0] via 192.168.40.1, 00:00:48
C       172.16.30.0 is directly connected, FastEthernet0/0
B       172.16.100.0 [20/0] via 192.168.40.1, 00:00:48
B    192.168.200.0/24 [20/0] via 172.16.30.2, 00:01:20
B    192.168.20.0/24 [20/0] via 192.168.30.2, 00:01:21
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
B       10.10.220.0/23 [20/0] via 192.168.40.1, 00:00:50
B       10.10.220.0/22 [20/0] via 172.16.30.2, 00:01:21
C    192.168.50.0/24 is directly connected, FastEthernet1/0
B    192.168.100.0/24 [20/0] via 192.168.50.1, 00:00:55
R3_AS30#
```

BGP最优路径选择

在默认情况下，到达同一目的地，BGP只走单条路径，并不希望在多条路径之间执行负载均衡。

BGP 的每条路由都带有路径属性，对于通过比较路径属性来选择最优路径，BGP 需要在多条路径之间按照一定的顺序比较属性，当多条路由的同一属性完全相同时，需要继续比较顺序中的下一条属性。直至选出最佳路由为止。

BGP路由选路原则

1. Weight属性
2. Local Preference属性
3. 本地路由始发方式
4. AS-Path长度
5. Origin属性
6. MED属性
7. EBGP优于IBGP
8. 到达Next-hop的代价
9. 执行等价负载均衡
10. EBGP路由接收的顺序
11. 路由的Router-ID
12. Cluster-list长度
13. 配置的BGP Peer指定地址

关于BGP路由器商业角色

出于经济利益的考虑，AS优先选择来自CustomerAS 的路由，其次是 PeerAS 及ProviderAS。换句话说，大部分网络采用的路由策略规则如下：

1. 来自 CustomerAS 宣告的路由允许传递给Customer、Peer 和 Provider。
2. 来自 PeerAS 宣告的路由允许传递给Customer，不允许通告给其他的 Peer 和 Provider。
3. 来自 ProviderAS 宣告的路由允许传递给Customer，不允许通告给其他的 Peer 和 Provider。

如下表：

Table 2 Routes Received from EBGP Peers

	Martian Address Space	Unallocated Address Space	Your AS Routes	Transit Routes	Private Peer Routes	Customer Routes
Transit Peers	✗	✗	✗	✓	✓	✓
Private Peers	✗	✗	✗	✗	✓	✗
Customers	✗	✗	✗	✗	✗	✓

PART 02

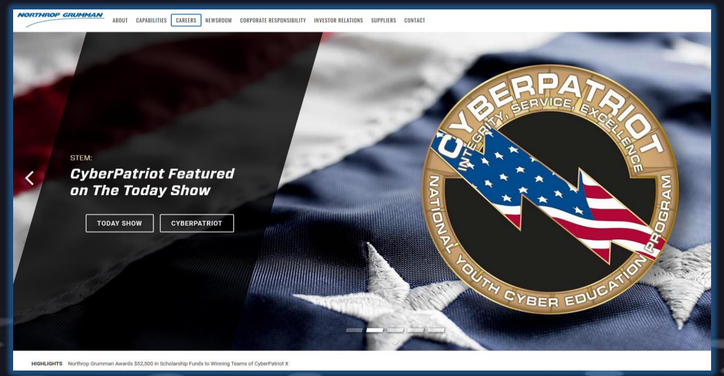
5个经典BGP安全大事件

There has never been a shortage of vivid BGP security incidents in history.Of course,we only selected five classic ones

5个经典的BGP安全大事件

Northrop Grumman部分bgp网络被恶意利用（2003）

2003年5月，一群垃圾邮件黑客攻击了美国诺斯洛普·格鲁门公司申请但（Northrop Grumman，当时世界第三大军工生产厂商、世界上最大的雷达制造商和最大的海军船只制造商）尚未使用的一段网络。并用来发送海量的垃圾邮件，以规避垃圾邮件过滤系统。最终，这家军火承包商花费2个月来重新声明对这些IP地址的所有权，并在国际互联网上封堵这些流氓路由广播。同时，由于被频繁地列入垃圾邮件地址黑名单，Northrop Grumman的IP地址全部被禁止使用。



巴基斯坦电信致YouTube断网事件（2008）

2008年2月，巴基斯坦政府以视频网站YouTube有亵渎神明内容为理由命令网络服务商封锁YouTube。巴基斯坦电信(Pakistan Telecom)试图限制本地用户接入YouTube，通过BGP向香港电信盈科（PCCW）发送新的路由信息（有错误）。然后PCCW向国际互联网广播了这个错误的路由信息。

当时，巴基斯坦电信在路由器上加了条static route把208.65.153.0/24弄到了null0接口（黑洞路由）;巴电信的工程师手抖把static route redistribute(Cisco路由器上同步不同协议路由表的方法)到BGP了，也就是说把该路由器上的静态路由表添加到BGP的路由表了，静态路由同步到其他路由表里的优先值最高。

BGP把这条路由向其他Peer AS的路由器同步了，最先中枪的是香港的电讯盈科（PCCW），然后接着被逐渐同步到了全世界。这时互联网的大部分用户想上Youtube的时候，数据包都丢到巴基斯坦某个路由器的null接口，结果当然是打不开。

5个经典的BGP安全大事件

Hacking Team利用BGP Hijack协助意大利黑客团体的攻击行动（2015）

利用bgp hijack技术劫持目标网络链路数据，然后结合Adobe flash 0day等技术手段向目标网络投递/植入RCS，完成长期监控。

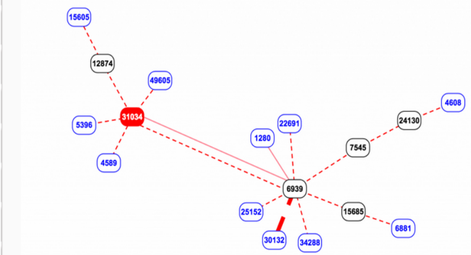
How Hacking Team Helped Italian Special Operations Group with BGP Routing Hijack

Posted by Andree Toonk - July 12, 2015 - Hijack - No Comments

By Andree Toonk and Dhia Mahjoub As part of the *Hacking Team* fall out and all the details published on Wikileaks, it became public knowledge that *Hacking Team* helped one of their customers Special Operations Group (ROS), regain access to Remote Access Tool (RAT) clients. As first reported here: http://blog.bofh.it/id_456 ROS recommended using BGP hijacking and *Hacking Team* helped with the setup of new RAT CnC servers. In this post we'll take a closer look at the exact details of this incident and support the Wikileaks findings with BGP data.

Raggruppamento Operativo Speciale and Hacking Team The *Raggruppamento Operativo Speciale* or ROS is the Special Operations Group of the Italian National Military police. The group focuses on investigating organized crime and terrorism. *Hacking Team* sells its RAT software known as Remote Control System (RCS) to law enforcement and intelligence agencies, ROS included. ROS infected and installed the RCS client on the machines of persons of interest (referred to in the emails as targets). These Remote Access Tools can provide ROS with all kinds of information and typically provide the tool's operator with full access over a victim's machine. The RCS clients normally need to check in with a server, which is a machine the clients can get their commands (orders) from and then upload stored data, recorded communications, logged keystrokes, etc., to. The Wikileaks emails uncovered how after ROS abruptly lost access to one of its RCS servers and worked together with *Hacking Team* to recover the loss. Initially, ROS used machines from a provider called Santrex, a well known bulletproof hoster. Brian Krebs dedicated an article about them in Oct 2013. Obviously the RCS clients (also referred to as agents in the Wikileaks emails) only work well if they can communicate with the server. If the server becomes unreachable the client essentially becomes an orphan and loses most of its value. This is exactly what happened on July 3rd, 2013 when after nine earlier outages that year, the Santrex IPv4 prefix *46.166.163.0/24* became permanently unreachable. The Wikileaks document described how the Italian ROS reached out to *Hacking Team* to work together on recovering the VPS server that ran on 46.166.163.175. In ROS terminology, the server was called "Anonymizer". The emails also revealed that this server relays updates to another back end server called "Collector" from

Wikileaks documents show how ROS worked with the Italian network operator AS31034 (aka Aruba S.p.A) to get the prefix announced in BGP and bring up a new "Anonymizer" server with the IP address 46.166.163.175. ROS also was hoping that other Italian ISPs wouldn't filter that hijacked announcement. When we look at historical BGP data we can confirm that AS31034 (Aruba S.p.A) indeed started to announce the prefix 46.166.163.0/24 starting on Friday, 16 Aug at 2013 07:32 UTC. The Wikileaks emails outline how ROS complained to *Hacking Team* that the IP was reachable only via Fastweb but not yet through Telecom Italia, concluding not all RCS clients were able to connect back to the server immediately, since the prefix was not seen globally. BGP data further confirms this per the visualization below.



BGPlay screenshot - BGP Network Graph for 46.166.163.0/24

5个经典的BGP安全大事件

Google工程师配置错误致日本800万用户断网1小时（2017）

Google工程师配置错误，意外劫持了NTT通信株式会社的流量。(NTT是日本一家主要的ISP，其还支持OCN和KDDI两个小型的ISP。在日本，NTT为767万家庭用户和48万家公司提供互联网服务)。导致日本持续断网40分钟左右，这在日本引起不小的恐慌。据日本当地媒体报道，日本总务省（Ministry of Internal Affairs and Communications）已经对此事展开调查，并要求ISP提供详细报告。

Google发言人发表声明承认是他们的错误，发言人向朝日新闻表示，Google对网络设置了错误信息导致问题发生，并对带来的不便与恐慌致以歉意。断网事件发生后，Google方面在8分钟之内更正了信息。

为什么日本会遭受如此严重的影响呢？

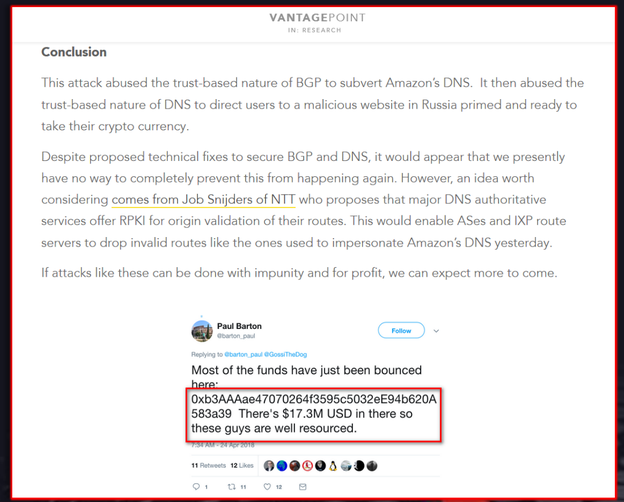
谷歌此次泄漏的16万条路由中，超过25,000条路由是属于NTT的路由地址段，在受影响的全部网络，涉及NTT的路由数最多。实际上，本次路由泄漏并不涉及KDDI的路由地址段。 但KDDI为何会遭此灾难呢？因为KDDI是Verizon的互联网转接（IP Transit）客户，也就是说，KDDI买了Verizon的互联网转接（IP Transit）服务。KDDI从Verizon接受了超过95,000条泄漏的路由前缀。日本另一个电信运营商IIJ也从Verizon接受了超过97,000条泄漏的路由前缀。因此，从KDDI或IIJ到NTT的任何互联网流量，都被先传送到谷歌在芝加哥的数据中心。NTT、KDDI、Softbank BB和IIJ是日本前四大互联网骨干网络，他们之间互联互通流量巨大。这次BGP路由事故导致其中三大日本运营商之间的国内流量国际化，漂洋过海跨越太平洋，经过日美之间众多国际海缆系统，流向谷歌的美国芝加哥数据中心。这种情况下，纵使日美之间国际海缆带宽原本很充足，也承载不了本来应该在日本国内的互联网洪荒之流，导致日美互联网高速公路严重堵塞，互联网流量通达时间过长，从而出现灾难性互联网数据丢包，导致日本互联网中断。

5个经典的BGP安全大事件

亚马逊遭BGP劫持致价值1730万美元ETH被盗（2018）

美国时间4月24号上午，亚马逊权威域名服务器遭到BGP路由劫持攻击。攻击者的目的是利用DNS和BGP固有的安全弱点来盗取加密货币。该劫持波及了澳洲、美国等地区。

本次事件中，用户对该网站的访问流量被全部劫持到一个俄罗斯ISP提供的非法网站。MyEtherWallet 已发声明表示很多用户成为本次攻击的受害者。



KCon

PART 03

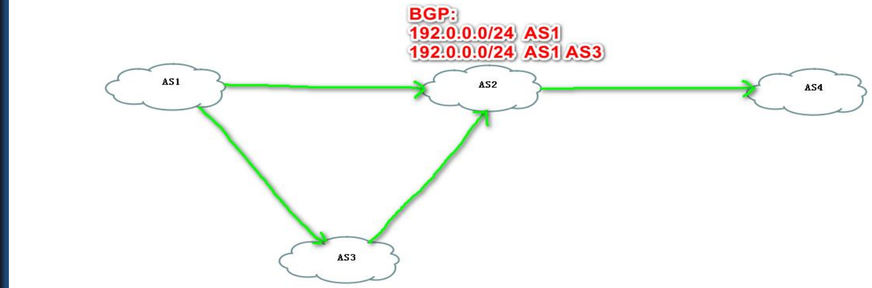
关于BGP的那些安全缺陷/漏洞

Security flaws or vulnerabilities regarding the BGP protocol.

BGP基本三原则

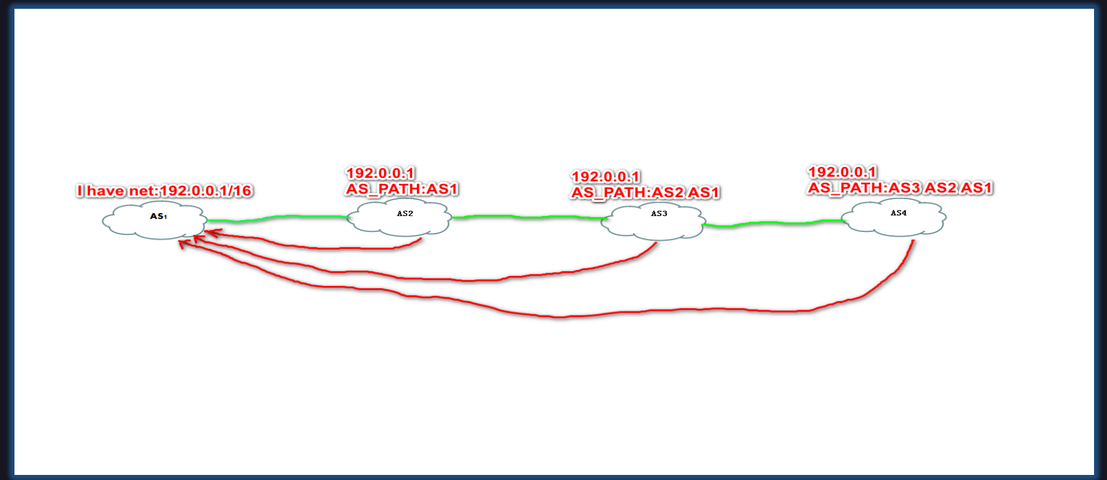
1、当BGP路由建立邻居连接后，彼此将路由条目发送给邻居。

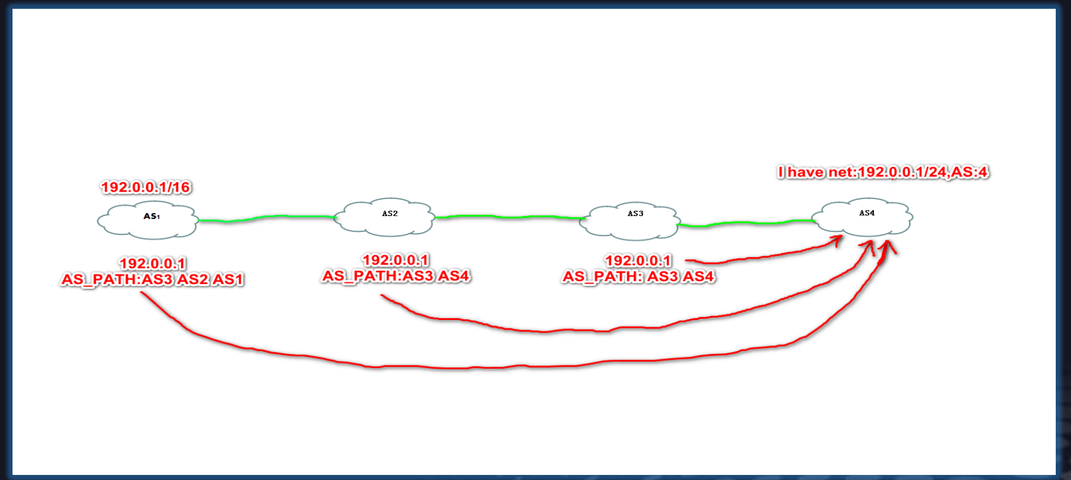
2、当目的网络确定时，AS_PATH最短路径具有路由优先权。



BGP基本三原则

3、当目的网络确定时，网络通告地址越具体(掩码越长)越有路由优先权。



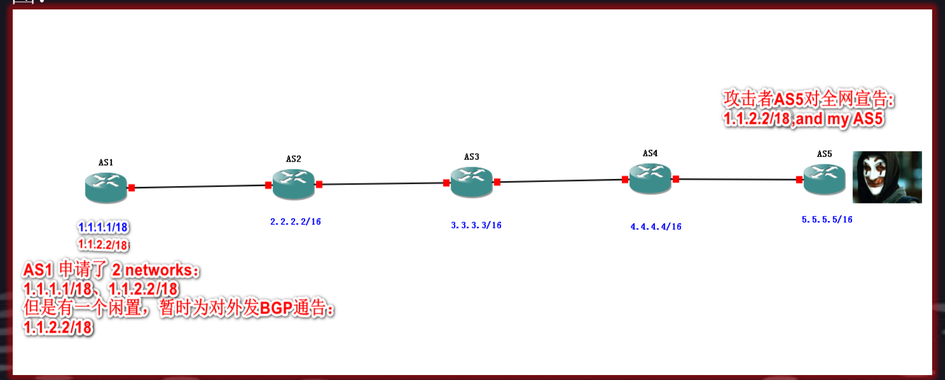


BGP hijack

- 闲置AS抢夺：
  对外宣告不属于自己，但属于其他机构合法且未被宣告的网络。

攻击前：

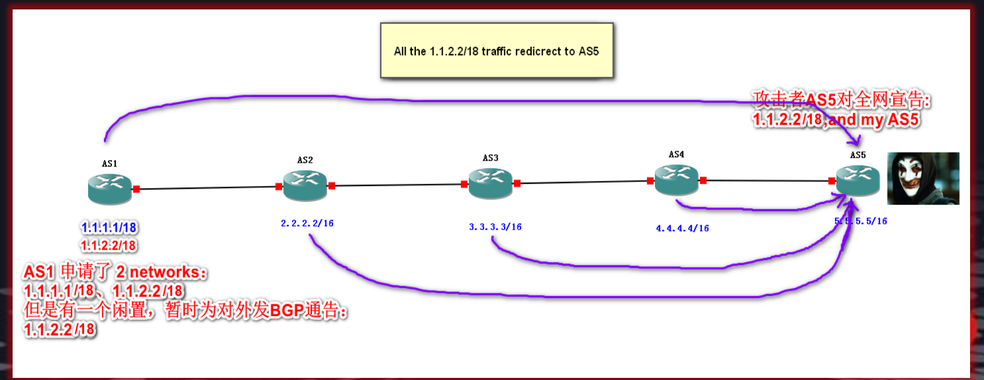
AS1是网络1.1.1.1/18和1.1.2.2/18的所有者，但其目前只使用了1.1.1.1/18，故对外只宣告了1.1.1.1/18，而没有宣告1.1.2.2/18。如下图：



攻击后：

AS5拥有网络5.5.5.5/16，他发现AS1没有对外宣告了1.1.2.2/18，而1.1.2.2/18确实是存在且是合法的。AS5对外宣告了1.1.2.2/18导致所有前往1.1.2.2/18的所有流量都发给了AS5。

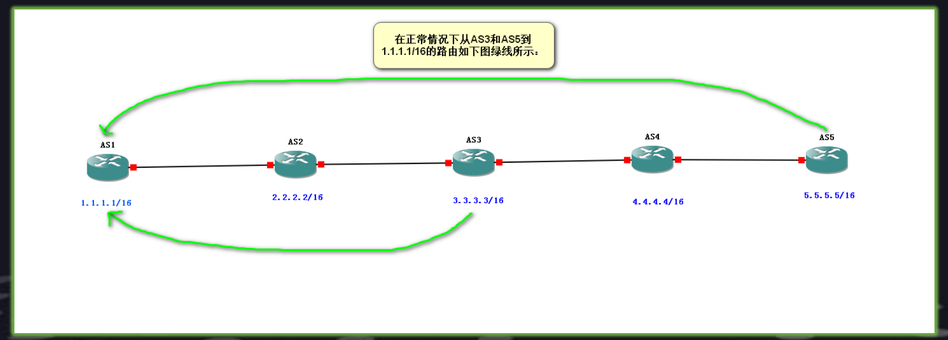
如下图：



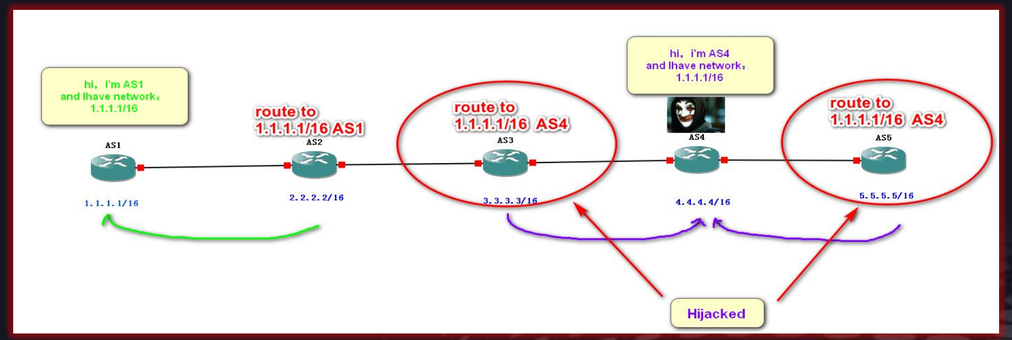
BGP hijack

- 近邻AS通告抢夺：
  利用物理位置邻近特性，就近宣告不属于自己的网络劫持近邻网络链路。

攻击前：



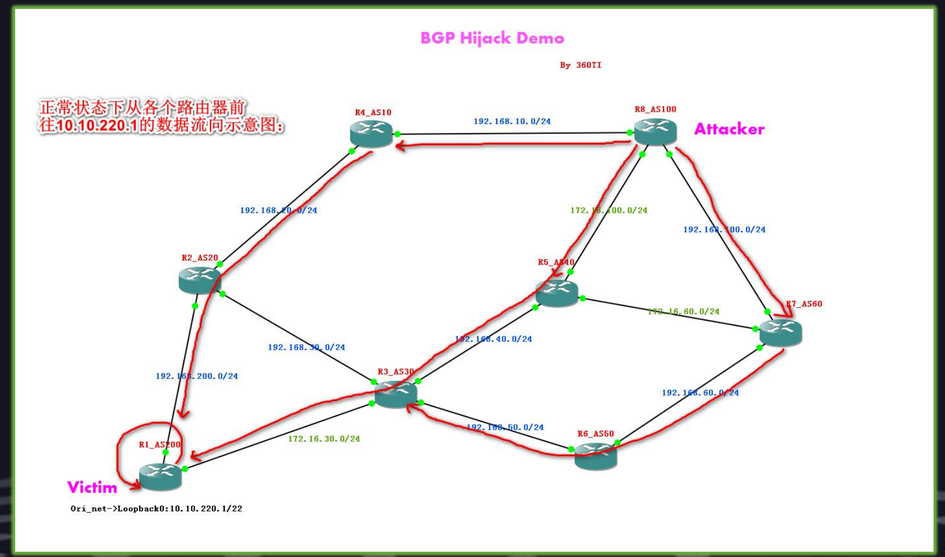
攻击后：



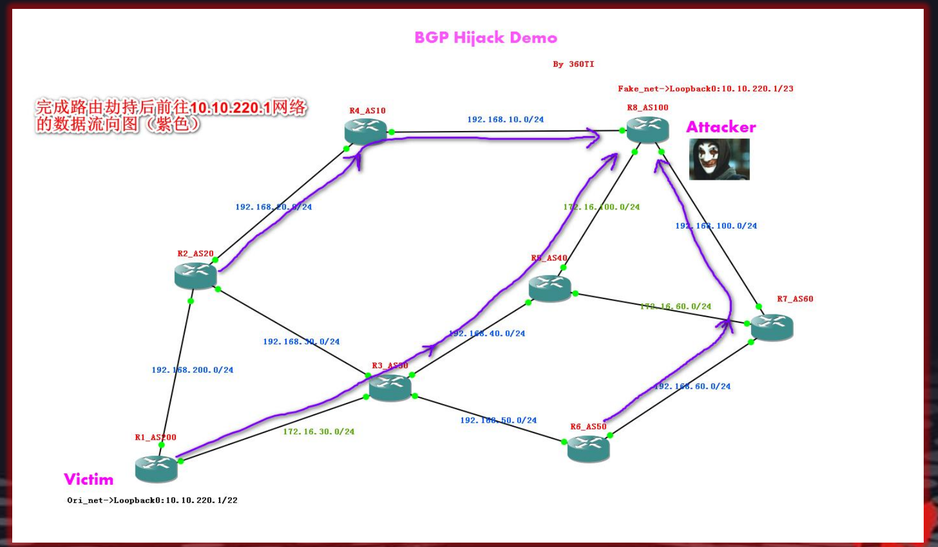
BGP hijack

- 长掩码抢夺（吸虹效应）Special-Prefix hijack：利用BGP选路长掩码优先的特性劫持所有可达网段全流量。

攻击前：



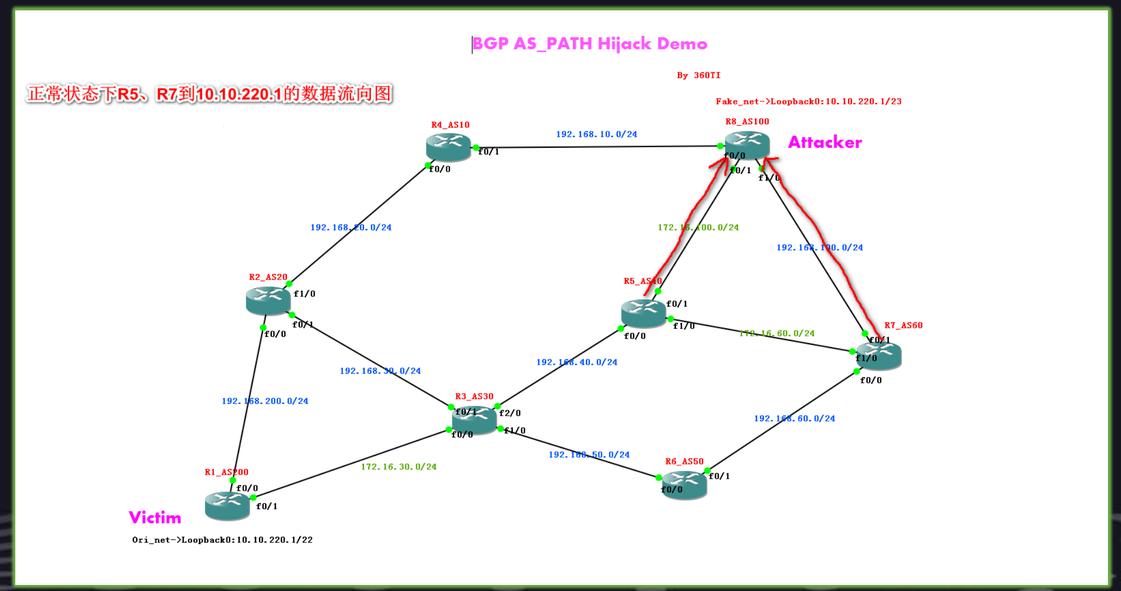
攻击后：



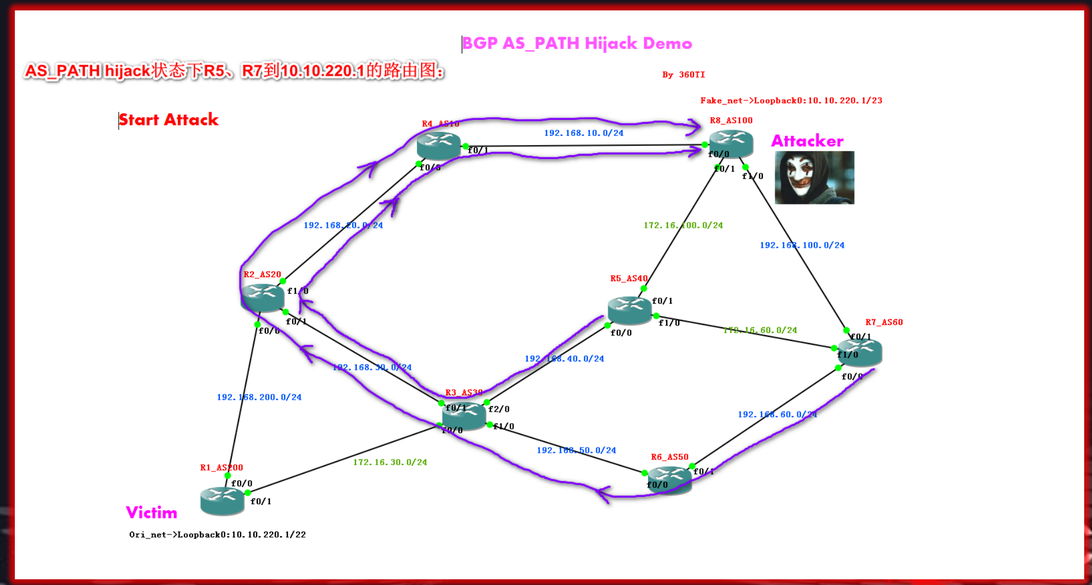
BGP hijack

- AS_PATH hijack (沙丁鱼捕术)：利用AS_PATH prepend可任意修改的特点,通过增加AS_PATH穿越AS数量抑制其路由优先级，将数据流向赶向目标网络。达到控制网络流量的目的。

攻击前：



攻击后：



路由泄露(Route leak)

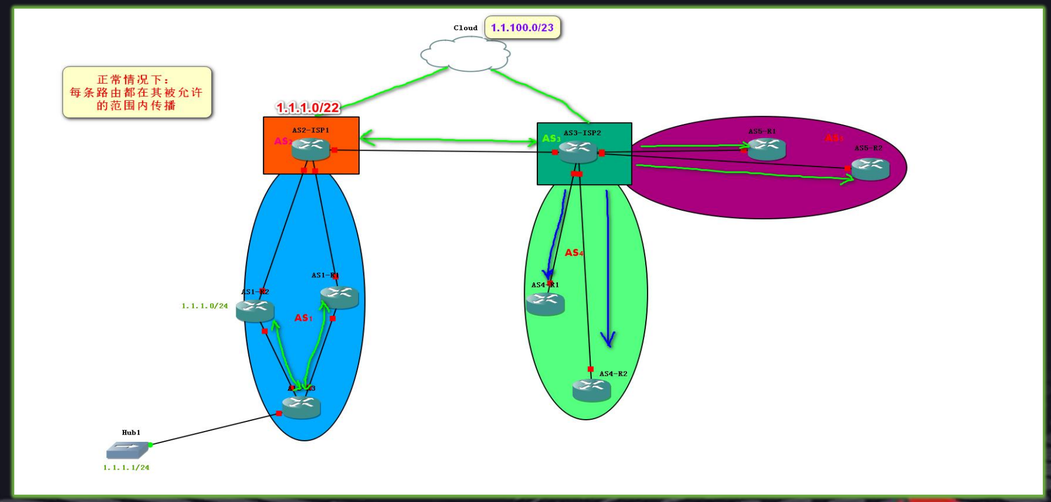
BGP路由泄露：

BGP路由条目在不同的角色都有其合理通告范围，一旦BGP路由通告传播到其原本预期通告范围之外称之为路由泄露，而这会产生难以准确预料的结果。

根据其发生泄漏后造成的结果大致可分为以下3种：

- 造成源网络中断。
- 造成源网络和被指向网络中断。
- 造成AS穿越/ISP穿越/MITM等问题。

在AS1发生路由泄露前，AS1、AS2、AS3、AS4、AS5都能正常通讯。如下图：



BGP TTL modify （饭后甜点）

EBGP运行在AS与AS之间的边界路由器上，默认情况下需要直连或使用静态路由。如果不是直连，必须指EBGP多条。否则无法建立邻居关系。为解决此问题定义了**ebgp-multihop**属性来修正跳数(hop)问题。在ebgp建立邻居的时候默认ttl值为1，如果不修改ebgp-multihop会导致非直连的ebgp邻居无法建立邻居关系（这也是一种ebgp的防环措施）。其实质就是**通过此属性来修改出站方向路由的TTL属性值**。

ebgp-multihop

To configure the exterior Border Gateway Protocol (eBGP) time-to-live (TTL) value to support eBGP multihop, use the **ebgp-multihop** command. To return to the default setting, use the **no** form of this command.

ebgp-multihop *ttl-value*

no ebgp-multihop *ttl-value*

Syntax Description

ttl-value	TTL value for eBGP multihop. The range is from 2 to 255. You must manually reset the BGP sessions after using this command.

Usage Guidelines

Use the **ebgp-multihop** command to configure the eBGP time-to-live (TTL) value to support eBGP multihop. In some situations, an eBGP peer is not directly connected to another eBGP peer and requires multiple hops to reach the remote eBGP peer. You can configure the eBGP TTL value for a neighbor session to allow these multihop sessions.

This command requires the LAN Enterprise Services license.

Examples

This example shows how to configure the eBGP multihop value:

```
switch(config)# router bgp 1.1

switch(config-router)# neighbor 192.0.2.1 remote-as 1.2

switch(config-route-neighbor) ebgp-multihop 2
```

BGP TTL值支持自定义修改，故可在进行MITM（BGP 路由TTL值每经过一跳值会减小1）攻击的同时制定策略，修改TTL值（增加对应跳数消耗的TTL值）让其跳数看起来无异常。能达到一定的隐藏作用。

switch(config)# router bgp 1.1

switch(config-router)# neighbor 192.0.2.1 remote-as 1.2

switch(config-route-neighbor) ebgp-multihop 2（1-255）

Use BGP Break HTTPS

有了之前的BGP hijack，现在只需拿到合法TLS证书即可解密https流量。

- 通过TLS CA 为用户获得TLS证书的过程如下：

1、先在CA网页申请一个帐号 ；
2、认证登录请求CSR（certificate signing request）创建并载入，尽管这很重要，一些CA甚至允许跳过这步直接从CA中取私钥；
3、CA提供了很多选择认证用户所有权，其中包含以下必备的3项：

查询whois记录
载入特定html在特定url通过认证
使用者在dns表中建立自定义token

4、当以上确认后，申请者付款。付款完成，CA发放TLS合法认证，然后我们就能用这个TLS证书向你网页访问者证明身份合法性。（确实是合法的，全球有效）

- 劫持CA（certificate authority）证书：

从以上过程我们可以看出，只要保证3中的3个条件验证通过，即可申请到合法的TLS证书。如果我们选择了正确的CA，BGP劫持打断CA间的通话也不会被发现。

实现这样的攻击你需要的只有两个

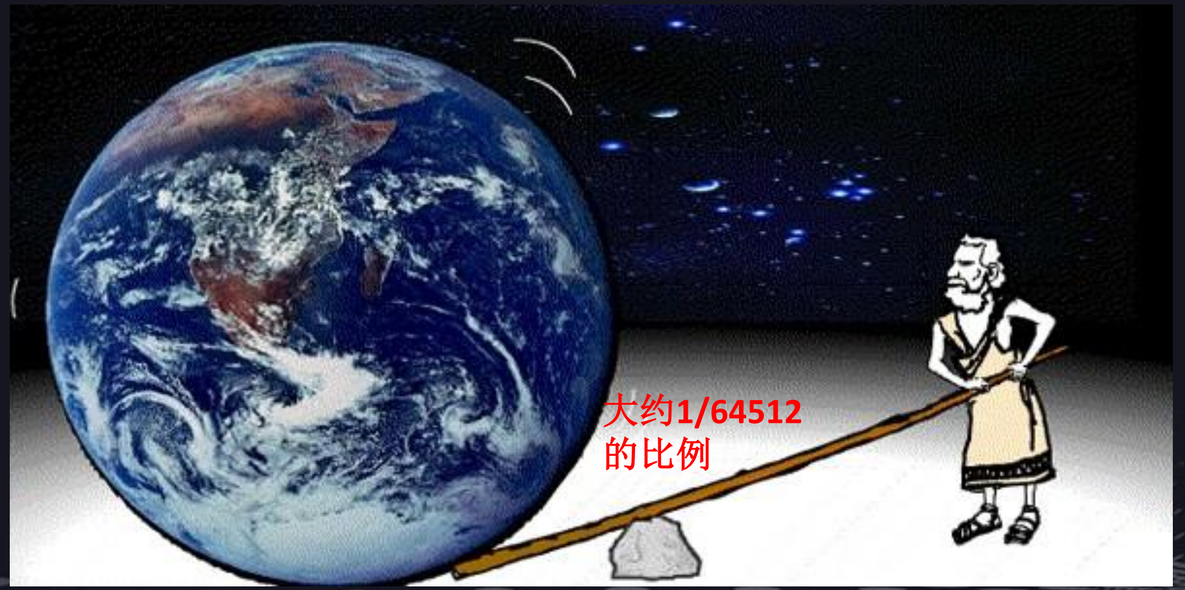
1、一个可控制的边界路由
2、你的BGP结点的信息：它的客户，提供者，结点信息，公共服务类似Qrator Radar或者 BGP监听。花一个小时确认这些基本信息，AS_PATH 追踪路线，等等。

然后：
使用BGP劫持技术将whios、URL认证server、DNS TXT、DNS token对应的地址指向自己搭建的3类server：

查询whois记录 （明文传送可伪造）
载入特定html在特定url通过认证 （明文传送可伪造）
使用者在dns表中建立自定义token （明文传送可伪造）
然后接着进行第4步即可完成TLS证书申请。

通过以上方法可拿到合法的TLS签名

给我一个合适的"支点"，我能撬动地球



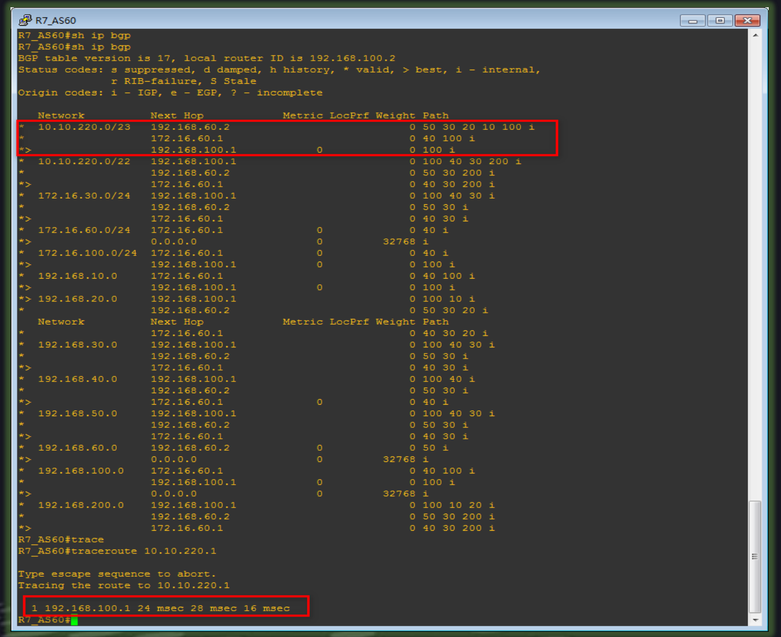
PART 04

检测 & 防御

How to detection and defense.

KCon

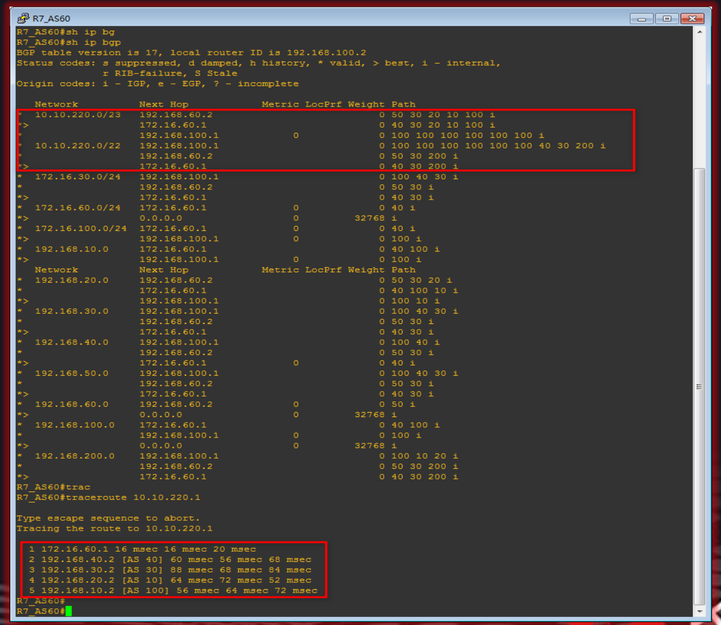
BGP Routes Moniting（检测篇）



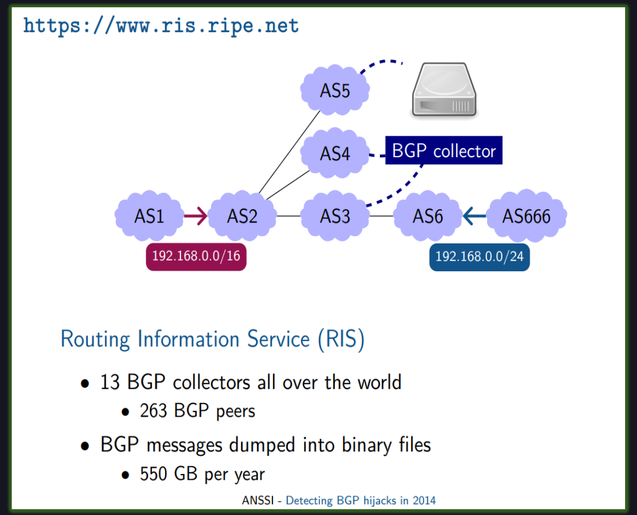
- 使用traceroute命令查看TTL相关信息。并与正常情况下进行比对。多数情况下可通过TTL值增减和经过的AS路径来判断是否存在劫持。

  当未发生路由劫持时，如下图：

当发生路由劫持时，发现路由绕行了：AS40->AS30->AS10->100。
如下图：



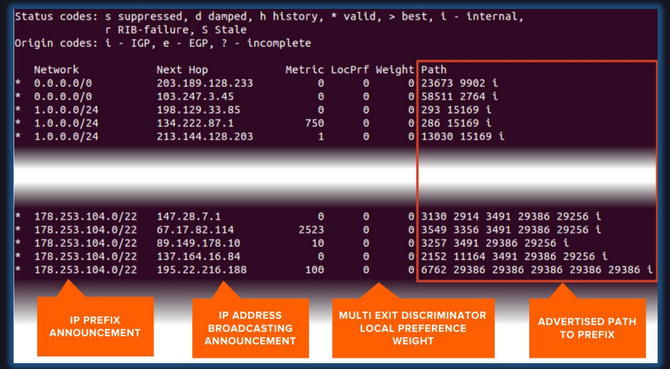
BGP Routes Moniting（检测篇）



- 自建平台实时同步全球权威机构、组织的全量BGP路由表，并与本地收集到的BGP进行比对。发现异常并实时告警。

  如下图：

  部分开源项目，如RouteViews：



- 选取合理的采集周期，在周期内对BGP正常状态下路由更新条目的数量进行统计。选取合理的更新条目总数阈值范围，实时监控AS内BGP路由条目更新数目，发现异常实时告警。

- 使用商业化BGP路由监控告警平台

  IAR (Internet Alert Registry)
  - PHAS (Prefix Hijack Alert System)
  - RIPE NCC MyASN Service
  - BGPmon
  - WatchMY.NET
  - Renesys Routing Intelligence

过滤和限制路由通告范围（防御篇）

- 梳理清楚AS范围内BGP、IGP全局路由策略哪些路由通告是允许的、哪些是禁止的。并合理使用ACL、Route-map或BGP Prefx Filtering控制路由的宣告、传播范围。
- 运营商、服务提供商应当依据以下原则，对不同商业角色路由器进行路由通告制定详细的BGP Prefx Filtering并启用。

如下图：

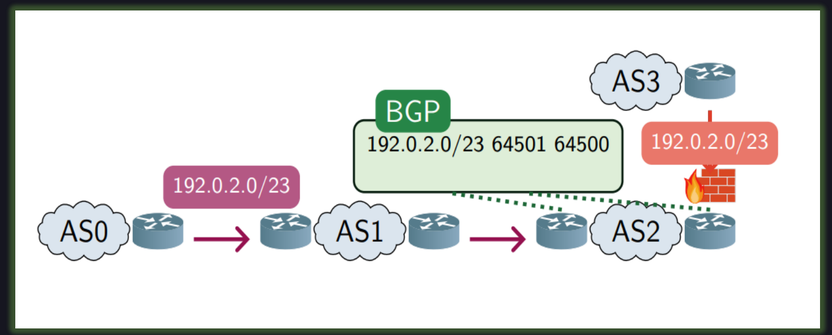
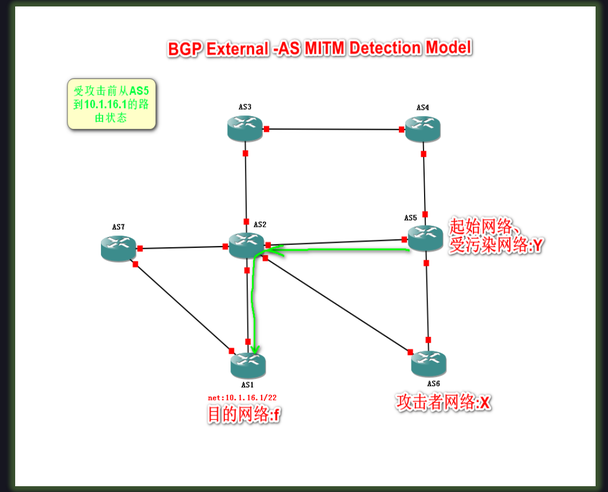


Table 2 Routes Received from EBGP Peers

	Martian Address Space	Unallocated Address Space	Your AS Routes	Transit Routes	Private Peer Routes	Customer Routes
Transit Peers	✗	✗	✗	✓	✓	✓
Private Peers	✗	✗	✗	✗	✓	✗
Customers	✗	✗	✗	✗	✗	✓

算法模型（检测篇---外部引用）

域间路由的中间人攻击模型



域间路由的中间人攻击通常基于前缀劫持来实现。前缀劫持宣告伪造的路由以劫持通往受害网络的流量。典型的前缀劫持如图所示。AS6向外非法宣告属于AS1的前缀10.1.16.1/22，使得AS4和AS5被该伪造路由污染。进而，它们到达受害网络AS1的流量也将被劫持到AS6中。如下图示：

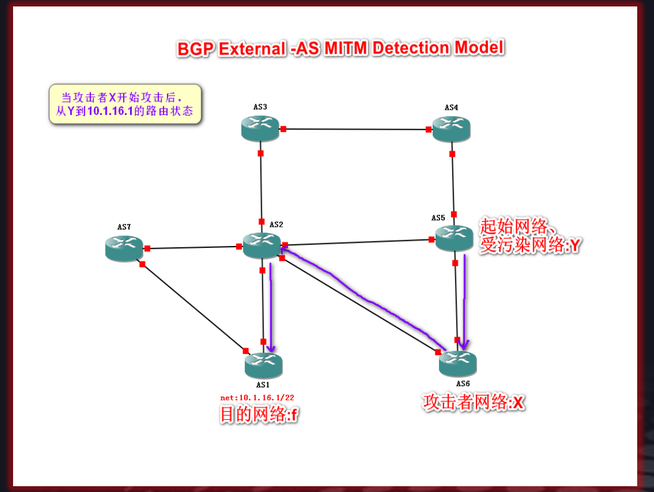
AS1是网络10.1.16.1/22的真实所有者，我们标示为:f

AS5为起始网络/受污染网络，我们标示为:Y

AS6为起始攻击者网络，我们标示为:X

在攻击发起前从Y到f的AS_PATH为：AS2 AS1。

在攻击发生后，从Y到f的AS_PATH为：AS6 AS2 AS1。如下图:



算法模型（检测篇---外部引用）

域间路由中间人攻击的异常特征

首先，如节上所述，域间路由中间人攻击的第1步是实施前缀劫持。鉴于前缀劫持会造成MOAS(multiple origin AS)冲突，因此**产生异常的MOAS是域间路由中间人攻击的第一个重要特征。**

由上述分析显见，除产生上述控制平面的MOAS异常外，域间路由中间人攻击还具有另外2个典型特征，即：

1）**受污染网络在攻击之后，其到达受害前缀的数据平面的转发路径比控制平面的AS-path要延长(换言之，控制平面的AS-path是其数据平面的转发路径的子路径)。**

2) **受污染网络在攻击之后到达受害前缀的转发路径的终点正是攻击之前到达该前缀的AS-path的终点。**

综合上面的分析，可使用公式表达式来描述：

故总结可知检测模型为：

Pb={b1，b2,…,bn} 表示**正常 AS-PATH**；

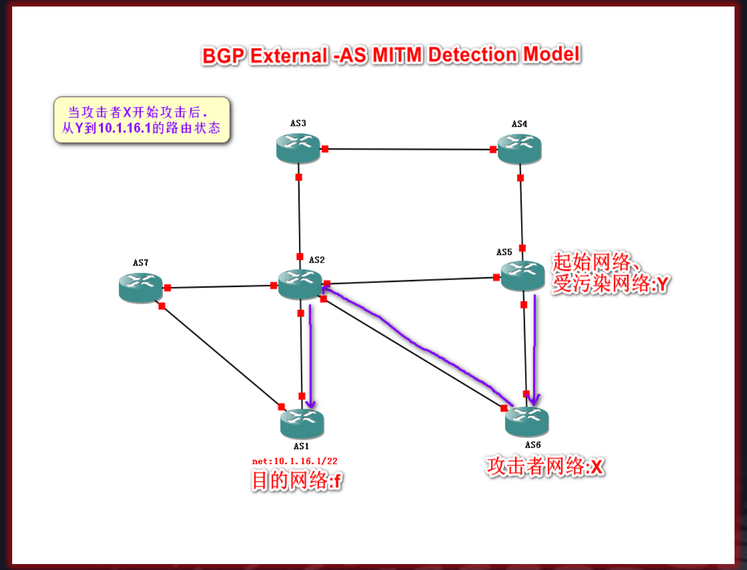
pa={a1，a2,…,am} 为攻击前后 AS Y（AS 5）被**污染的 AS-PATH**；

Wf={c1，c2,…,ck} 为攻击后 AS Y（AS 5）到达 f（AS 1）的**数据包绕行转发路径**；

$$\{am \neq bn\}$$

$$\{k-m \geqslant 1;\ ci=ai\ ;1 \leqslant i \leqslant m\}$$

$$\{ck=bn\}$$



安全增强协议RPKI 与BGPsec （终极防御篇）

- RPKI（RFC 6810）

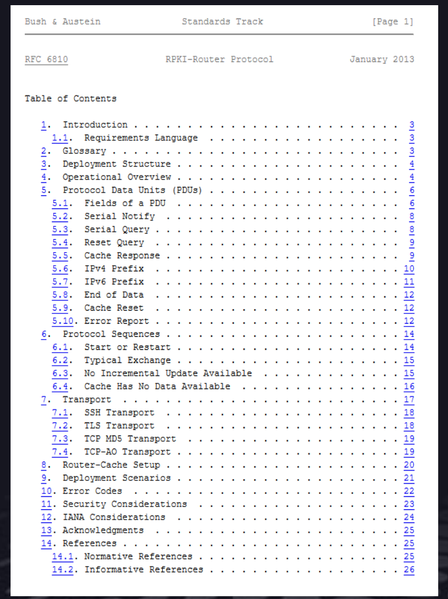
针对BGP路由前缀劫持问题，当前业界正在推进的方案是RPKI（Resource Public Key Infrastructure:互联网码号资源公钥基础设施）。
在之前亚马逊的案例中，当天上午为时两小时的过程中，攻击者（AS10297）对以下前缀发起了路由起源声明：

205.251.192.0/24, AS10297
205.251.193.0/24, AS10297
205.251.195.0/24, AS10297
205.251.197.0/24, AS10297
205.251.199.0/24, AS10297

如果亚马逊部署RPKI并签发资源证书和ROA（路由起源认证），那么其他部署了RPKI路由器的自治网络就可以帮助过滤这些虚假路由。
具体地说，亚马逊使用自己的RPKI证书签发以下ROA并发布到全球资料库中：

<205.251.192.0/23, AS16509>
<205.251.193.0/23, AS16509>
<205.251.195.0/23, AS16509>
<205.251.197.0/23, AS16509>
<205.251.199.0/23, AS16509>

那么部署了RPKI路由器的其他自治网络，就可以从RPKI依赖方那里得到验证后的IP前缀和起源AS号的绑定关系，继而判定起源于AS16509的相应路由通告为真并将其保留，以及判定由攻击者发起的起源于AS10297的路由通告为假并将其丢弃，从而完全抵御这次路由劫持。
RPKI作为一种域间路由安全机制，本身只能提供路由起源认证，而不能提供路由全路径认证，所以RPKI能够避免以上这种前缀劫持攻击。



Bush & Austein Standards Track [Page 1]

RFC 6810 RPKI-Router Protocol January 2013

Table of Contents

➢ BGPsec（RFC 8206）

但其他类型的路由攻击（如路由泄漏攻击和路径缩短攻击）可以绕过RPKI进行流量劫持。针对这种情况，IETF提出了一种部署在RPKI之上的全路径认证机制——BGPsec，并将其标准化。BGPsec要求每一个AS都对它接收到的路由通告消息进行签名，签名内容作为路由消息的路径属性BGPsec_Path_Signatures通告给邻居AS。

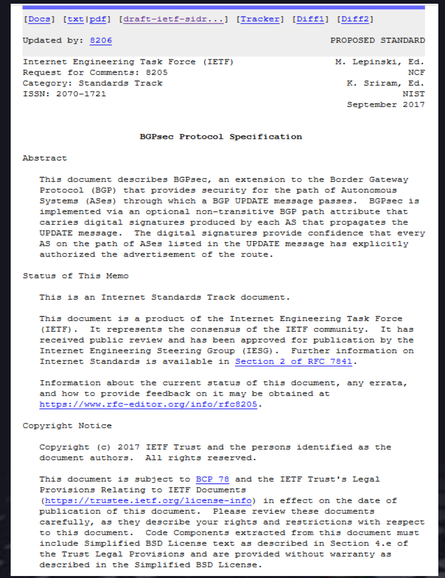
签名内容包括：

(1)上一个AS的BGPsec_Path_Signatures；
(2)本自治系统的AS号；
(3)路由消息要发往的自治网络的AS号；
(4)本AS的RPKI路由器公钥。

由此可见，BGPsec_Path_Signatures实际上代表了AS路径中的前一AS对后一AS继续通告该路由的授权。

部署了BGPsec的AS在路径签名之前还要进行路径验证，验证过程如下：

当一个AS收到路由通告消息后，会依次验证AS路径中每一个AS对应的BGPsec签名（包含在BGPsec_Path_Signatures中）。如果全部验证成功，说明该AS路径是真实有效的，当前AS才可能采用并继续向外广播该路由通告。BGPsec可以有效避免BGP路径缩短攻击。



[Docs] [txt|pdf] [draft-ietf-sidr...] [Tracker] [Diff1] [Diff2]

Updated by: 8206 PROPOSED STANDARD

Internet Engineering Task Force (IETF) M. Lepinski, Ed.
Request for Comments: 8205 NCF
Category: Standards Track K. Sriram, Ed.
ISSN: 2070-1721 NIST
September 2017

BGPsec Protocol Specification

Abstract

This document describes BGPsec, an extension to the Border Gateway Protocol (BGP) that provides security for the path of Autonomous Systems (ASes) through which a BGP UPDATE message passes. BGPsec is implemented via an optional non-transitive BGP path attribute that carries digital signatures produced by each AS that propagates the UPDATE message. The digital signatures provide confidence that every AS on the path of ASes listed in the UPDATE message has explicitly authorized the advertisement of the route.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8205.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

PART 05

BGP,AT&T and NSA

Say good,but you exchange the CARDS under the table

KCon

棱镜门始。末...

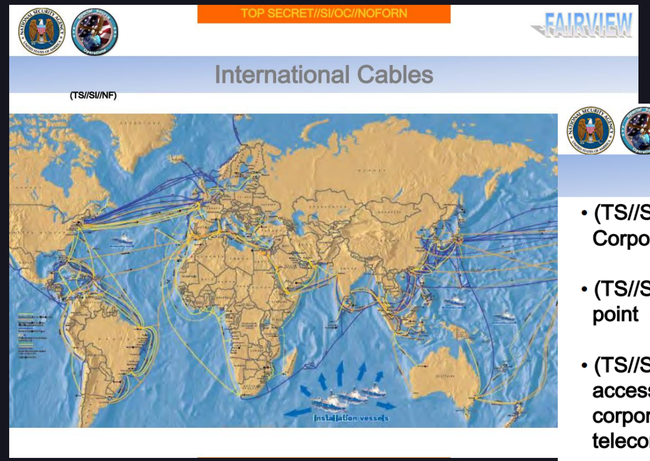
说好的不出老千，你却桌底换牌.....

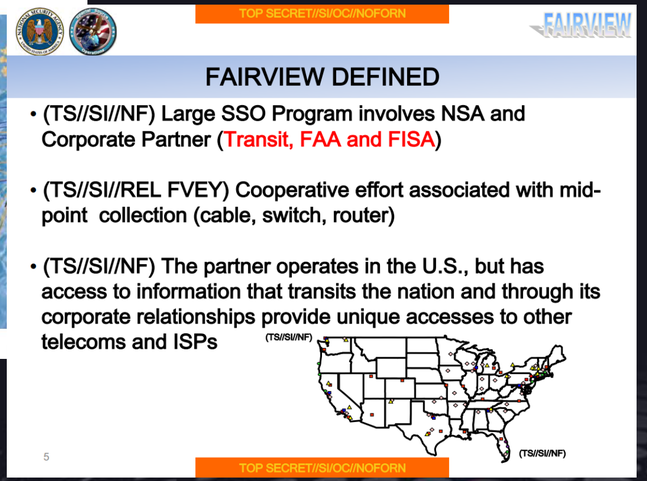
棱镜计划（PRISM）是一项由美国国家安全局（NSA）自2007年起开始实施的绝密电子监听计划。该计划的正式名号为“US-984XN”。

揭秘者德华·斯诺登曾是美国中央情报局技术分析员，《华盛顿邮报》说，斯诺登之前是国家安全局设在夏威夷的威胁行动中心的系统管理员，更早曾替中情局工作。斯诺登爆料称，美国政府随时可以读取任何人的电邮，令包括谷歌在内的网络巨头致函美国政府自清，他还称美国政府已入侵中国大陆与香港特区的网络多年。

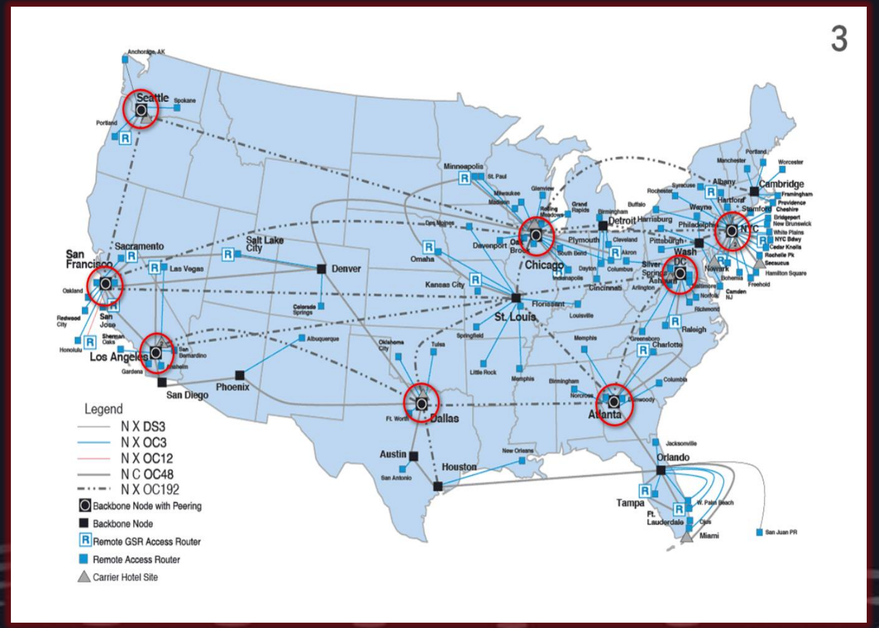
泄露的文件中描述PRISM计划能够对即时通信和既存资料进行深度的监听。许可的监听对象包括任何在美国以外地区使用参与计划公司服务的客户，或是任何与国外人士通信的美国公民。国家安全局在PRISM计划中可以获得的数据电子邮件、视频和语音交谈、影片、照片、VoIP交谈内容、档案传输、登入通知，以及社交网络细节。综合情报文件“总统每日简报”中在2012年内在1,477个计划使用了来自PRISM计划的资料。

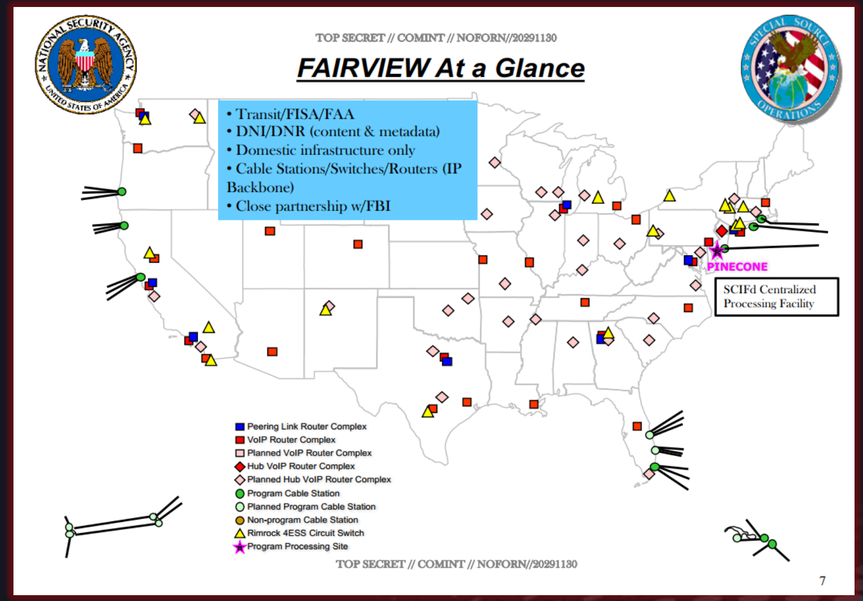
泄露的数据显示，自2009年以来，美国已针对中国网络发动了大规模的入侵活动。攻击目标达到数百个之多，其中还包括学校。据悉，美国政府黑客主要通过入侵巨型路由器从而一举入侵成千上万台电脑，而不是分别入侵每一台电脑。





基础设施建设篇



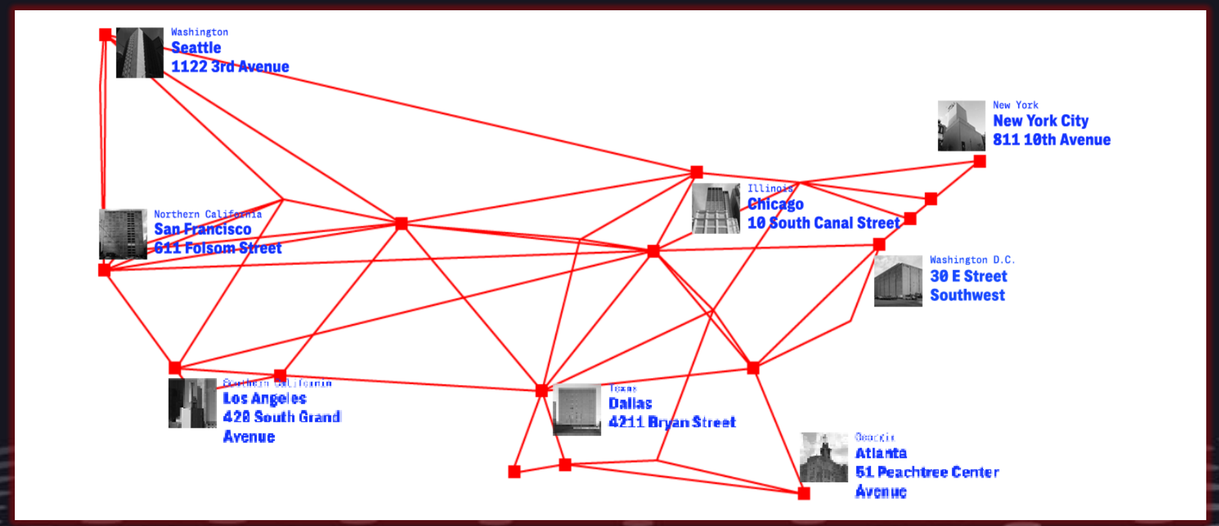


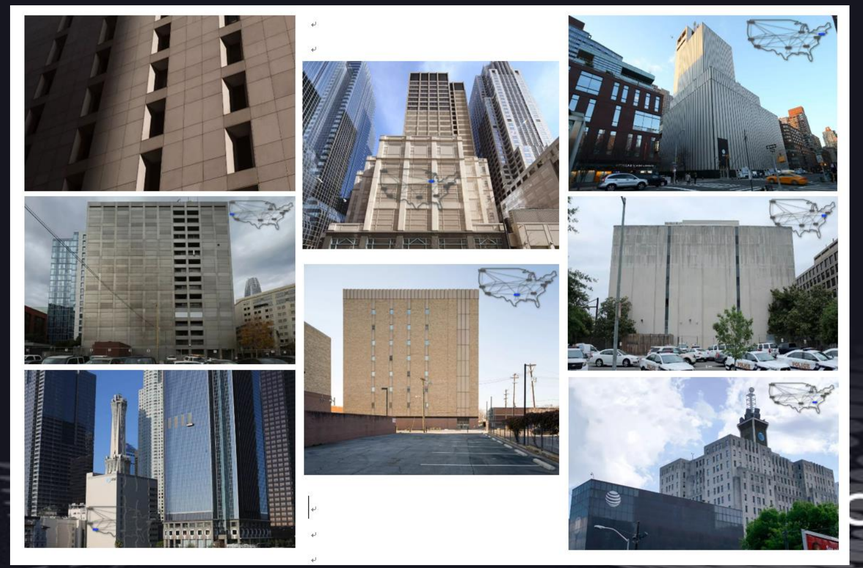
BGP,AT&T and NSA

基础设施建设篇

美国国家安全局（NSA）的秘密据点隐藏在美国各地的城市中，那些高耸的没有窗户的摩天大楼和足以抵御地震，甚至核攻击。成千上万的人每天经过这些建筑物，很少再给他们看第二眼，因为他们的功能并未公开。它们是全球最大的电信网络中不可分割的一部分，它们也与有争议的国家安全局监视计划相关。

亚特兰大，芝加哥，达拉斯，洛杉矶，纽约，旧金山，西雅图和华盛顿特区。截讯网在以上每个城市都确定了一个AT&T的设施，其中的网络设备可以截获美国传输大量的互联网数据。一系列证据（包括国家安全局的文件，公共记录以及与多名前美国电报电话公司员工的访谈） 都表明，这些建筑物是国家安全局间谍活动的核心，多年来一直监控数十亿封通过美国的电子邮件，电话和在线聊天。(可靠消息来源theintercept.com)

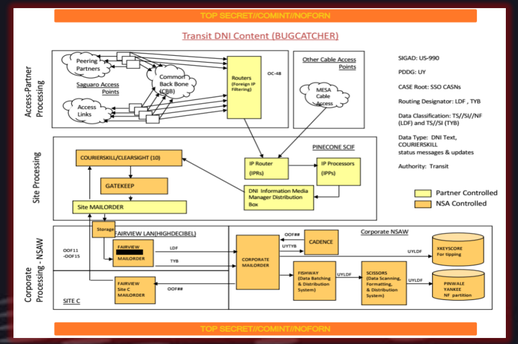




BGP,AT&T and NSA

技术可行性

➢ 战略层面技术点可行性：
在恰当节点先通过BGP Prefix hijack、BGP AS_PATH hijack、HTTPS TLS hijack等技术控制目标网络流量，然后分而治之

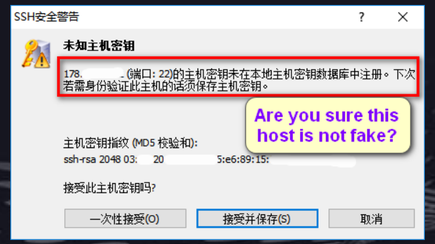


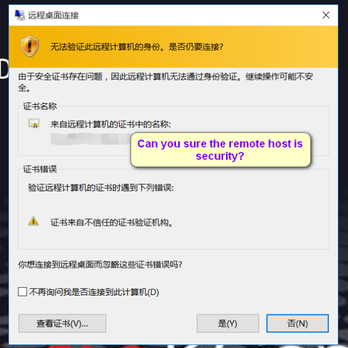
➢ 战术层面技术点可行性：
衔接上一环节的分类流量，并针对不同具体类型的流量制定与之对应的后续处理流程。例如：

明文监听：
ftp、http、telnet、http、smtp、snmp、pop、pop3、VoIP、UPnP…
明文传输数据不解释。

加密通讯信任关系降级攻击：
ssh、https（tls hijack）、3389（RDP）、VNC…
第一步client至server端信任关系欺骗。后面的都可以依靠假证书或信任关系解密数据。

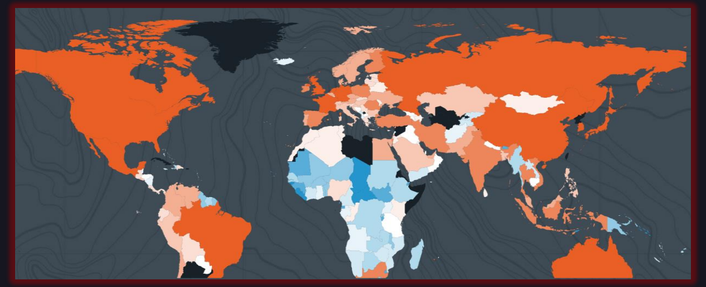
加密数据通讯监听：
ssh、https、mssql、mysql、Oracle Datebase、DB2、3389（RD
实时监听密文数据包，必要时调用超算资源破解。





我国互联网节点通讯安全现状

网络安全公司 Rapid7 近日发布的《2018国家暴露指数报告》显示，全球端口暴露最严重的十个国家为美国、中国、加拿大、韩国、英国、法国、荷兰、日本、德国和墨西哥，其中美国暴露的情况最严重，中国位列第二，仅次于美国。



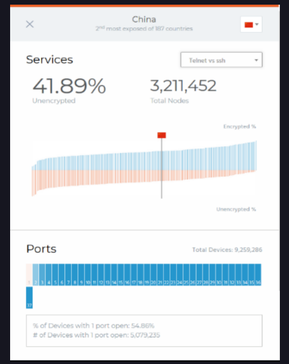
中国1400万服务器暴露原因

中国有超过3.4亿个 IPv4 地址，Rapid7 的研究人员发现中国有约1400万台服务器对扫描有响应。

报告指出，中国暴露严重的主要原因在于缺乏加密服务，这使被动的监控和针对不安全明文协议的主动攻击成为可能。从这方面来看，中国的 Web 服务器数量远不及其他国家，且加密 Web 的比率为26%，远远低于 Rapid7 期望的35%。

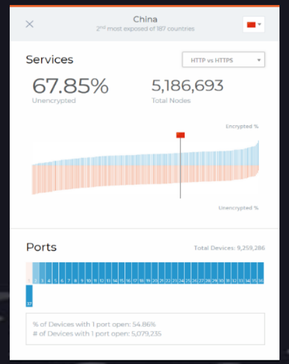
Rapid7 指出，由于中国人倾向于使用中国托管的网站，而非国际托管服务，因此这一点会带来麻烦。同样，中国的加密 Shell 比率为58%，远远低于与之经济实力相当国家的平均水准（75%），更易遭受类似 Mirai 僵尸网络的攻击。

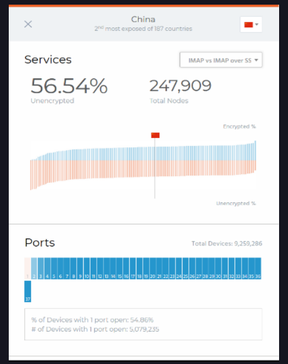
我国互联网节点通讯安全现状



Telnet VS SSH

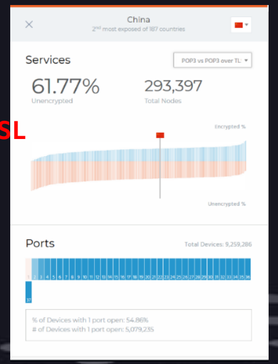
HTTP VS HTTPS

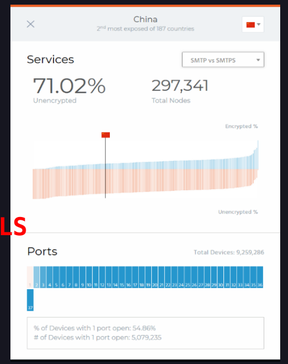




IMAP VS IMAP over SSL

POP3 VS POP3 over TLS





SMTP VS SMTPS

总体概况综述：

1、引用的数据反映了现状态下我国暴露在外的互联网的节点数世界第二,仅次于美国。

2、这些暴露在外的数据超过50%是没有加密的。（50%+）

3、以上还没有算上加密协议漏洞、可进行加密通讯信任关系降级攻击和软硬件级别供应链攻击手段影响的范围。

我国互联网节点通讯安全现状

总体概况综述：

近几年来虽然IETF已经有RPKI、BGPsec等安全的BGP标准推出,但由于种种原因（硬件资源消耗、迭代成本、过度风险等）这些标准的推进部署进度依旧十分缓慢。

所以要有一个清晰的认识：

BGP在未来的5至10年内依然不是安全的

谢谢观看

演讲人：张玉兵(Eric)

360威胁情报中心

个人交流微信