blog.cloudflare.com

Deep Inside a DNS Amplification DDoS Attack

14-18 minutes

\

A few weeks ago I wrote about DNS Amplification Attacks. These attacks are some of the largest, as measured by the number of Gigabits per second (Gbps), that we see directed toward our network. For the last three weeks, one persistent attacker has been sending at least 20Gbps twenty-four hours a day as an attack against one of our customers.

That size of an attack is enough to cripple even a large web host. For CloudFlare, the nature of our network means that the attack, which gets diluted across all of our global data centers, doesn't cause us harm. Even from a cost perspective, the attack doesn't end up adding to our bandwidth bill because of the way in which we're charged for wholesale bandwidth.

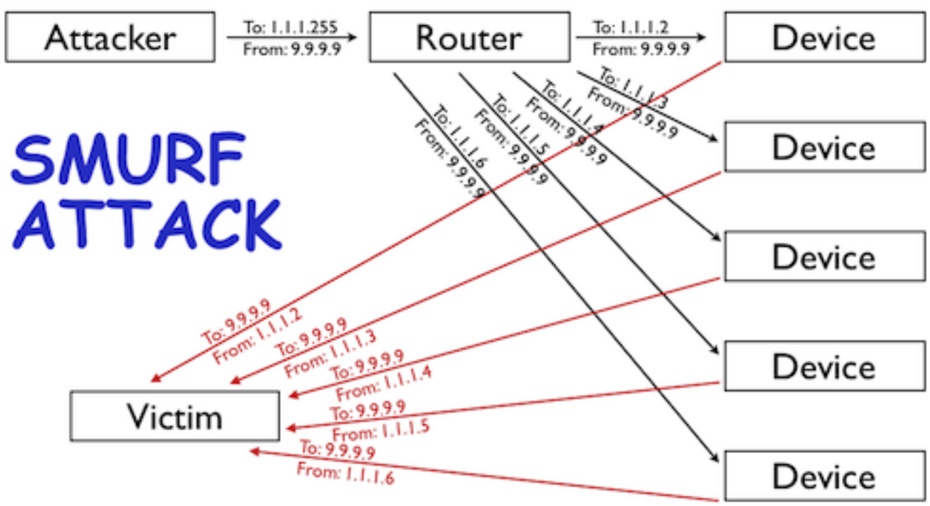
We buy a lot of bandwidth and we pay for the higher of our ingress (in-bound) or egress (out-bound) averaged over a month. Since we act as a caching proxy, under normal circumstances egress always exceeds ingress. When there's an attack, the two lines get closer together but rarely is an attack large enough to add to our overall bandwidth costs.

Given that the latest attack wasn't impacting us or any of our customers, we decided to let it run for a while and see what we could learn.

Amplification Attacks

DNS Amplification Attacks are a way for an attacker to magnify the amount of bandwidth they can target at a potential victim. Imagine you are an attacker and you control a botnet capable of sending out 100Mbps of traffic. While that may be sufficient to knock some sites offline, it is a relatively trivial amount of traffic in the world of DDoS. In order to increase your attack's volume, you could try and add more compromised machines to your botnet. That is becoming increasingly difficult. Alternatively, you could find a way to amplify your 100Mbps into something much bigger.

The original amplification attack was known as a SMURF attack. A SMURF attack involves an attacker sending ICMP requests (i.e., ping requests) to the network's broadcast address (i.e., X.X.X.255) of a router configured to relay ICMP to all devices behind the router. The attacker spoofs the source of the ICMP request to be the IP address of the intended victim. Since ICMP does not include a handshake, the destination has no way of verifying if the source IP is legitimate. The router receives the request and passes it on to all the devices that sit behind it. All those devices then respond back to the ping. The attacker is able to amplify the attack by a multiple of how ever many devices are behind the router (i.e., if you have 5 devices behind the router then the attacker is able to amplify the attack 5x, see the diagram below).



SMURF attacks are largely a thing of the past. For the most part, network operators have configured their routers to not relay ICMP requests sent to a network's broadcast address. However, even as that amplification attack vector has closed, others remain wide open.

DNS Amplification

There are two criteria for a good amplification attack vector: 1) query can be set with a spoofed source address (e.g., via a protocol like ICMP or UDP that does not require a handshake); and 2) the response to the query is significantly larger than the query itself. DNS is a core, ubiquitous Internet platform that meets these criteria and therefore has become the largest source of amplification attacks.

DNS queries are typically transmitted over UDP, meaning that, like ICMP queries used in a SMURF attack, they are fire and forget. As a result, their source attribute can be spoofed and the receiver has no way of determining its veracity before responding. DNS also is capable of generating a much larger response than query. For example, you can send the following (tiny) query (where x.x.x.x is the IP of an open DNS resolver):

```
dig ANY isc.org @x.x.x.x
```

And get back the following (gigantic) response:

```
; <<>> DiG 9.7.3 <<>> ANY isc.org @x.x.x.x
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR,
id: 5147
;; flags: qr rd ra; QUERY: 1, ANSWER: 27,
AUTHORITY: 4, ADDITIONAL: 5

;; QUESTION SECTION:
;isc.org.                        IN        ANY

;; ANSWER SECTION:
isc.org.                4084        IN        SOA
ns-int.isc.org. hostmaster.isc.org. 2012102700
```

```
7200 3600 24796800 3600
isc.org.                4084     IN      A
149.20.64.42
isc.org.                4084     IN      MX
10 mx.pao1.isc.org.
isc.org.                4084     IN      MX
10 mx.ams1.isc.org.
isc.org.                4084     IN      TXT
"v=spf1 a mx ip4:204.152.184.0/21
ip4:149.20.0.0/16 ip6:2001:04F8::0/32
ip6:2001:500:60::65/128 ~all"
isc.org.                4084     IN      TXT
"$Id: isc.org,v 1.1724 2012-10-23 00:36:09 bind
Exp $"
isc.org.                4084     IN      AAAA
2001:4f8:0:2::d
isc.org.                4084     IN      NAPTR
20 0 "S" "SIP+D2U" "" _sip._udp.isc.org.
isc.org.                484      IN      NSEC
_kerberos.isc.org. A NS SOA MX TXT AAAA NAPTR
RRSIG NSEC DNSKEY SPF
isc.org.                4084     IN
DNSKEY       256 3 5
BQEAAAAB2F1v2HWzCCE9vNsKfk0K8vd4EBwizNT9KO6WYXj0oxEL4eOJ
aXbax/BzPFx+3qO8B8pu8E
/JjkWH0oaYz4guUyTVmT5Eelg44Vb1kssy
q8W27oQ+9qNiP8Jv6zdOj0uCB/N0fxfVL3371xbednFqoECfSFDZa6Hw
jU1qzveSsW0=
isc.org.                4084     IN
DNSKEY       257 3 5
```

```
BEAAAAOhHQDBrhQbtphgq2wQUpEQ5t4DtUHxoMVFu2hWLDMvoOMRXjGr
hhCeFvAZih7yJHf8ZGfW6hd38hXG/xylYCO6Krpbdojwx8YMXLA5/kA+
u50WIL8ZR1R6KTbsYVMf/Qx5RiNbPClw+vT+U8eXEJmO20jIS1ULgqy3
47cBB1zMnnz/4LJpA0da9CbKj3A254T515sNIMcwsB8/2+2E63
/zZrQz
Bkj0BrN/9Bexjpiks3jRhZatEsXn3dTy47R09Uix5WcJt+xzqZ7+ysyI
KOOedS39Z7SDmsn2eA0FKtQpwA6LXeG2w+jxmw3oA8lVUgEf/rzeC/bE
yBNsO70aEFTd
isc.org.                4084    IN      SPF
"v=spf1 a mx ip4:204.152.184.0/21
ip4:149.20.0.0/16 ip6:2001:04F8::0/32
ip6:2001:500:60::65/128 ~all"
isc.org.                484     IN      RRSIG
NS 5 2 7200 20121125230752 20121026230752 4442
isc.org. oFeNy69Pn+/JnnltGPUZQnYzo1YGglMhS
/SZKnlgyMbz+tT2r/2v+X1j
AkUl9GRW9JAZU+x0oEj5oNAkRiQqK+D6DC+PGdM2/JHa0X41LnMIE2NX
UHDAKMmbqk529fUy3MvA/ZwR9FXurcfYQ5fnpEEaawNS0bKxomw48dcp
Aco=
isc.org.                484     IN      RRSIG
SOA 5 2 7200 20121125230752 20121026230752 4442
isc.org.
S+DLHzE/8WQbnSl70geMYoKvGlIuKARVlxmssce+MX6DO
/J1xdK9xGac
XCuAhRpTMKElKq2dIhKp8vnS2e+JTZLrGl4q/bnrrmhQ9eBS7IFmrQ6s
0cKEEyuijumOPlKCCN9QX7ds4siiTIrEOGhCaamEgRJqVxqCsg1dBUrF
hKk=
isc.org.                484     IN      RRSIG
MX 5 2 7200 20121125230752 20121026230752 4442
isc.org.
```

```
VFqFWRPyulIT8VsIdXKMpMRJTYpdggoGgOjKJzKJs/6ZrxmbJtmAxgEu
/rkwD6Q9JwsUCepNC74EYxzXFvDaNnKp/Qdmt2139h
/xoZsw0JVA4Z+b
zNQ3kNiDjdV6zl6ELtCVDqj3SiWDZhYB/CR9pNno1FAF2joIjYSwiwbS
Lcw=
isc.org.                484         IN         RRSIG
TXT 5 2 7200 20121125230752 20121026230752 4442
isc.org.
Ojj8YCZf3jYL9eO8w4Tl9HjWKP3CKXQRFed8s9xeh5TR3KI3tQTKsSeI
JRQaCXkADiRwHt0j7VaJ3xUHa5LCkzetcVgJNPmhovVa1w87Hz4DU6q9
k9bbshvbYtxOF8xny/FCiR5c6NVeLmvvu4xeOqSwIpoo2zvIEfFP9deF
UhA=
isc.org.                484         IN         RRSIG
AAAA 5 2 7200 20121125230752 20121026230752 4442
isc.org. hutAcro0NBMvKU/m+2lF8sgIYyIVWORTp
/utIn8KsF1WOwwM2QMGa5C9
/rH/ZQBQgN46ZMmiEm4LxH6mtaKxMsBGZwgzUEdfsvVtr+fS5NUoA1rF
wg92eBbInNdCvT0if8m1Sldx5/hSqKn8EAscKfg5BMQp5YDFsllsTauA
8Y4=
isc.org.                484         IN         RRSIG
NAPTR 5 2 7200 20121125230752 20121026230752 4442
isc.org.
ZD14qEHR7jVXn5uJUn6XR9Lvt5Pa7YTEW94hNAn9Lm3Tlnkg11AeZiOU
3woQ1pg+esCQepKCiBlplPLcag3LHlQ19OdACrHGUzzM+rnHY50Rn/H4
XQTqUWHBF2Cs0CvfqRxLvAl5AY6P2bb/iUQ6hV8Go0OFvmMEkJOnxPPw
5i4=
isc.org.                484         IN         RRSIG
NSEC 5 2 3600 20121125230752 20121026230752 4442
isc.org.
rY1hqZAryM045vv3bMY0wgJhxHJQofkXLeRLk20LaU1mVTyu7uair7jk
```

```
MwDVCVhxF7gfRdgu8x7LPSvJKUl6sn731Y80CnGwszXBp6tVpgw6oOcr
Pi0rsnzC6lIarXLwNBFmLZg2Aza6SSirzOPObnmK6PLQCdmaVAPrVJQs
FHY=
isc.org.                484         IN        RRSIG
DNSKEY 5 2 7200 20121125230126 20121026230126 4442
isc.org. i0S2MFqvHB3wOhv2IPozE/IQABM
/eDDCV2D7dJ3AuOwi1A3sbYQ29XUd
BK82+mxxsET2U6hv64crpbGTNJP3OsMxNOAFA0QYphoMnt0jg3OYg+AC
L2j92kx8ZdEhxKiE6pm+cFVBHLLLmXGKLDaVnffLv1GQIl5YrIyy4jiw
h0A=
isc.org.                484         IN        RRSIG
DNSKEY 5 2 7200 20121125230126 20121026230126
12892 isc.org.
j1kgWw+wFFw01E2z2kXq+biTG1rrnG1XoP17pIOToZHElgpy7F6kEgyj
fN6e2C+gvXxOAABQ+qr76o+P+ZUHrLUEI0ewtC3v4HziMEl0Z2/NE0MH
qAEdmEemezKn9O1EAOC7gZ4nU5psmuYlqxcCkUDbW0qhLd+u/8+d6L1S
nlrD/vEi4R1SLl2bD5VBtaxczOz+2BEQLveUt
/UusS1qhYcFjdCYbHqF
JGQziTJv9ssbEDHT7COc05gG+A1Av5tNN5ag7QHWa0VE+Ux0nH7JUy0N
ch1kVecPbXJVHRF97CEH5wCDEgcFKAyyhaXXh02fqBGfON8R5mIcgO/F
DRdXjA==
isc.org.                484         IN        RRSIG
SPF 5 2 7200 20121125230752 20121026230752 4442
isc.org.
IB/bo9HPjr6aZqPRkzf9bXyK8TpBFj3HNQloqhrguMSBfcMfmJqHxKyD
ZoLKZkQk9kPeztau6hj2YnyBoTd0zIVJ5fVSqJPuNqxwm2h9HMs140r3
9HmbnkO7Fe+Lu5AD0s6+E9qayi3wOOwunBgUkkFsC8BjiiGrRKcY8GhC
kak=
isc.org.                484         IN        RRSIG
A 5 2 7200 20121125230752 20121026230752 4442
```

```
isc.org.
ViS+qg95DibkkZ5kbL8vCBpRUqI2/M9UwthPVCXl8ciglLftiMC9WUzq
Ul3FBbri5CKD/YNXqyvjxyvmZfkQLDUmffjDB+ZGqBxSpG8j1fDwK6n1
hWbKf7QSe4LuJZyEgXFEkPl6CmVyZCTITUh2TNDmRgsoxrvrOqOePWhp
8+E=
isc.org.            4084    IN      NS
ns.isc.afilias-nst.info.
isc.org.            4084    IN      NS
ams.sns-pb.isc.org.
isc.org.            4084    IN      NS
ord.sns-pb.isc.org.
isc.org.            4084    IN      NS
sfba.sns-pb.isc.org.

;; AUTHORITY SECTION:
isc.org.            4084    IN      NS
ns.isc.afilias-nst.info.
isc.org.            4084    IN      NS
ams.sns-pb.isc.org.
isc.org.            4084    IN      NS
ord.sns-pb.isc.org.
isc.org.            4084    IN      NS
sfba.sns-pb.isc.org.

;; ADDITIONAL SECTION:
mx.ams1.isc.org.    484     IN      A
199.6.1.65
mx.ams1.isc.org.    484     IN      AAAA
2001:500:60::65
mx.pao1.isc.org.    484     IN      A
```

```
149.20.64.53
mx.pao1.isc.org.        484         IN          AAAA
2001:4f8:0:2::2b
_sip._udp.isc.org.      4084        IN          SRV
0 1 5060 asterisk.isc.org.

;; Query time: 176 msec
;;SERVER: x.x.x.x#53(x.x.x.x)
;; WHEN: Tue Oct 30 01:14:32 2012
;; MSG SIZE  rcvd: 3223
```

That's a 64 byte query that resulted in a 3,223 byte response. In other words, an attacker is able to achieve a 50x amplification over whatever traffic they can initiate to an open DNS resolver. Note, ironically, how the effectiveness of the attack based on the size of the response is made worse by the inclusion of the huge DNSSEC keys -- a protocol designed to make the DNS system more secure.

Open DNS Resolvers: Bane of the Internet

The key term that I used a couple times so far is "open DNS resolver." The best practice, if you're running a recursive DNS resolver is to ensure that it only responds to queries from authorized clients. In other words, if you're running a recursive DNS server for your company and your company's IP space is 5.5.5.0/24 (i.e., 5.5.5.0 - 5.5.5.255) then it should only respond to queries from that range. If a query
arrives from 9.9.9.9 then it should not respond.

The problem is, many people running DNS resolvers leave them open and willing to respond to any IP address that queries them. This is a known problem that is at least 10 years old. What has happened recently is a number of distinct botnets appear to have enumerated the Internet's IP space in order to discover open resolvers. Once discovered, they can be used to launch significant DNS Amplification Attacks.

If you look at the geographic data on attack origins, the US dominates the list, but that is largely skewed by the number of networks present within the country. Per capita, the worst country is Taiwan where the country's HINET is the second largest source of open resolvers of any network in the world. We've also published a list of the top networks from which we're seeing abused open DNS resolvers. Below is a sample of the top-ten worst offenders:

# of Open Resolvers	AS Number	Network Name
3359	45595	PKTELECOM-AS-PK Pakistan Telecom Company Limited
2992	3462	HINET Data Communication Business Group
1431	9394	CRNET CHINA RAILWAY Internet(CRNET)
1403	21844	THEPLANET-AS - ThePlanet.com Internet Services, Inc.
1323	4134	CHINANET-BACKBONE No.31, Jin-rong Street
1120	36351	SOFTLAYER - SoftLayer Technologies Inc.
1112	4713	OCN NTT Communications Corporation
1039	26496	AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC

# of Open Resolvers	AS Number	Network Name
980	7018	ATT-INTERNET4 - AT&T Services, Inc.
852	32613	IWEB-AS - iWeb Technologies Inc.

------------------------- --------------- ---

Wonder why there's been an increase in big DDoS attacks? It's in large part because the network operators listed above have continued to allow open resolvers to run on their networks and the attackers have begun abusing them. While we're reluctant to publish the list of the actual IP address of the open resolvers for fear that they may be misused, if you are one of the operators of one of the networks listed above, we're happy to share data with you in order to help you get your network cleaned up. Organizations such as Team Cymru publish [more extensive lists] and also work with
network operators to get their networks cleaned up.

If you are running an open recursor, you should close it now. Leaving it open means you will continue to aid in these attacks. If you're running BIND, you can include one or more of the following in your configuration file in order to limit attackers abusing your network:

```
// Disable recursion for the DNS service
//options {    recursion no;};

// Permit DNS queries for DNS messages with source
addresses
// in the 192.168.1.0/24 netblock. The 'allow-
query-cache'
// options configuration can also be used to limit
```

```
the IP
// addresses permitted to obtain answers from the
cache of
// the DNS server. Substitute with your own
network range.
//options {    allow-query {192.168.1.0/24;};};
```

CloudFlare itself is designed to automatically learn from the traffic to our network, whether the traffic is good or bad. While this size of attack would be crippling for most networks, it has been relatively trivial for us to identify the sources of the attack, route them so they don't affect any of our customers, and study their behavior over the last three weeks. Now that we've enumerated the sources of the attack, we've begun to null route the traffic upstream to fully neuter the attack.

We will continue to work with the networks listed above in order to get their networks cleaned up. And, as new threats emerge, we'll continue to share information on them in order to ensure the Internet can remain fast and safe.