Surviving a DDoS Attack:

Securing CDN traffic at CloudFlare

NETNOD Autumn 2014
October 2, 2014

Martin J. Levy, Network Strategy
www.cloudflare.com
DDoS Attacks are becoming massive, and easier to initiate
Major Attacks against CloudFlare Customers

- **Feb 2012**: 65 Gbps
- **Mar 2013**: 309 Gbps
- **Feb 2014**: 400 Gbps
- **Next?**: ??? Gbps

---

2 Oct 2014

NETNOD Autumn 2014 - CloudFlare - Surviving a DDoS Attack - Securing CDN traffic at CloudFlare
CloudFlare
CloudFlare core locations
CloudFlare sample customers
1.5+ million customers
Chronology of the major attacks
March 2013
The Spamhaus attack
Monday, March 18th thru 21st

“Annoyance” attacks, 10-80Gbps
Wednesday, March 20th

“Instant on”

~75Gbps attack
Then, it got real ...
Sunday, March 24th thru 25th

“Instant on”

Peaks of the attack reached 309Gbps
February 2014
Monday, February 10th, 2014

400Gbps, Globally Distributed Attacks
and here's what it looks like when a device participates in the NTP DDOS against @CloudFlare

4:53 PM - 12 Feb 2014

36 RETWEETS 10 FAVORITES
Breaking Down the Attacks
DDoS mechanics
IP Spoofing

Attacker
9.8.7.6

Hi, I’m 1.2.3.4, and I need this info

Network Server

Here’s your info

1.2.3.4
IP Spoofing

http://spoofer.cmand.org/

25.5% of networks allow spoofing
Attack #1 – Spamhaus Attack:

309 Gbps
UDP
DNS
Getting to 309Gbps

10 Mbps × 30,900 = 309,000 Mbps
An easier way: DNS Amplification

Attacker 64 Bytes

Open DNS Resolver

3,363 Bytes

~50x

Target Website
How easy is it to create a query packet?
64 bytes becomes 3,363 bytes

$ dig ANY isc.org @63.21*...* +edns=0 +notcp +bufsize=4096

$
300Gbps+ of DDoS attack traffic

1 laptop
+ 5-7 compromised servers
+ 3 networks which allow spoofing
+ 9Gbps of DNS requests to
+ 0.1% of all open resolvers

= 300Gbps of DDoS attack traffic
Attack #2 – The NTP Attack:
400Gbps UDP NTP
Tweets report attack issues

Retweeted by Stéphane Bortzmeyer

Octave Klaba / Oles @olesovhcom · Feb 12
We see today lot of new DDoS attacks from Internet to our network. Type: NTP
AMP Size: >350Gbps. No issue. VAC is great :)

Expand

Brian Carpenter @geeknik · Feb 14
This script will let you create a DDOS attack using NTP servers
buff.ly/1bwDTKH

Expand

Matthew Prince @eastdakota · Mar 5
Encouraging: China Mobile reached out to clean up 231 vulnerable NTP servers
on their network. ~5% those involved in 400Gbps DDoS attack.

Expand
An EVEN easier way: NTP Amplification

Attacker

64 Bytes

NTP Server with MONLIST

13,184 Bytes

~206x

Target Website
400Gbps+ of DDoS attack traffic

1 laptop
+ 1 compromised server
+ 1 network which allowed spoofing
+ 1.94Gbps of MONLIST to

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

= 400Gbps+ of DDoS attack traffic
What’s Next?

- DNS → 8x
- EDNS → ~50x
- NTP → ~206x
- SNMP → 650x
Protecting your network
28 Million Open DNS Resolvers

Open Resolver Project

Open Resolvers pose a significant threat to the global network infrastructure by answering recursive queries for hosts outside of its domain. They are utilized in DNS Amplification attacks and pose a similar threat as those from Smurf attacks commonly seen in the late 1990s.

We have collected a list of 32 million resolvers that respond to queries in some fashion. 28 million of these pose a significant threat (as of 27-OCT-2013). Detailed History and Breakdown

Check my IP space

Search my IP space (eg: 192.0.2.0/24 - searches "larger" than /22 will be rejected): 127.0.0.0/24

ipv4-heatmap of 20130519 data heatmap archive

What can I do?

If you operate a DNS server, please check the settings.

Recursive servers should be restricted to your enterprise or customer IP ranges to prevent abuse. Directions on securing BIND and Microsoft nameservers can be found on the Team CYMRU Website. If you operate BIND, you can deploy the TCP-ANY patch.

Authoritative servers should not offer recursion, but can still be used in an attack. Configure your Authoritative DNS servers to use DNS RRL [Response Rate Limiting] Knot DNS and NLNetLabs NSD include this as a standard option now. BIND requires a patch.

CPE DEVICES SHOULD NOT listen for DNS packets on the WAN interface, including NETWORK and BROADCAST addresses.

Prevent spoofing on your network!

Configure Source Address Validation/uRPF/BCP-38 on all CPE and Datacenter equipment edges that have fixed IP ranges. This could be as simple as setting ip verify unicast source reachable-via rx on a router interface. Any statically routed customer should receive this setting by default.

If you are in the security community:

Please contact dns-scan /at/ puck.nether.net for access to raw data.

Additional Information

Informações em Português

We can provide you a List of Open Resolvers by ASN if you e-mail dns-scan /at/ puck.nether.net

Test your IP Now!

DNS DDoS and Security in the News

- 04-APR-2013 Spamhaus DDoS was just a warning shot
- 30-MAR-2013 How the Cyberattack on Spamhaus Unfolded
- 20-MAR-2013 Is Your DNS Server part of a criminal conspiracy?
- 20-MAR-2013 750Gb/s DDoS against Cloudflare

Presentations:

- DNS-QARC May 2013 - slides
- NANOG 58 June 2013 - Lightning Talk

Lock your DNS server (recursive & authoritative) down
28 Million Open DNS Resolvers

UNIX bind configuration examples

```
options {
    recursion no;
    additional-from-cache no;
};

acl "trusted" {
    10.42.0.0/16;
    192.0.2.0/24;
    192.0.6.0/24;
};
options {
    recursion no;
    additional-from-cache no;
    allow-query { none; }
};
view "trusted" in {
    match-clients { trusted; }
    allow-query { trusted; }
    recursion yes;
    additional-from-cache yes;
};
```

Confirm that the resolver is a closed resolver
NTP Amplification Attacks

OpenNTPProject.org - NTP Scanning Project

Search my IP space (eg: 192.0.2.0/24 - searches "larger" than /22 will be rejected): 127.0.0.0/24

If you are a member of the general public:

How can I check my server? - run the command `ntpd -n -c monlist 192.0.2.1` or `ntpq -c rv 192.0.2.1` - if you see a response, your server may be used in attacks.

How can I fix my server, router or other device? You should upgrade to NTP-4.2.7p26 or later. You can add `disable monitor` to your `ntp.conf` and restart your NTP process if on an earlier version. Also check out the [Team Cytrus Secure NTP Template](http://TeamCytrus.org/). Also see [NTP Bug #1532](http://bugs.ntp.org);

The server should also not respond to `loopinfo` or `iostats` requests as well.

We test the internet for NTP MODE 6 and MONLIST MODE 7 responses.

Cisco customers should ask about or open a case against [CSCum44673](http://cisco.com).

Recent News:
- 2014-02-22 - Amplification Hell: Revisiting Network Protocols for DDoS Abuse
- 2014-02-13 - Technical Details behind 400Gb/s NTP attack
- 2014-01-13 - 100Gb/s attacks using NTP
- 2013-12-26 - Christmas 2013 NTP Attacks

If you are a member of the security community:

You can contact the ntp-scan /at/ puck.nether.net to obtain the raw data. It is available for re-use in your reporting.

About US:

OpenNTPProject.org is operated in conjunction with Network Time Foundation. If this service is valuable, please consider joining or donating to NTF.

Turn off MONLIST on your NTP servers
NTP Amplification Attacks

Number of vulnerable servers

Graph showing the decrease in the number of vulnerable servers over time.

@jaredmauch
NTP MONLIST Amplifiers down from 490k -> 349k in the last week.
OpenNTPProject.org to check your network.
11:50 PM - 14 Feb 2014
24 RETWEETS 6 FAVORITES
NTP Amplification Attacks

UNIX ntpd configuration example

`# by default act only as a basic NTP client`  
`restrict -4 default nomodify nopeer noquery notrap`  
`restrict -6 default nomodify nopeer noquery notrap`  
`# allow NTP messages from the loopback address, useful for debugging`  
`restrict 127.0.0.1`  
`restrict -6 ::1`  
`# server(s) we time sync to`  
`server 192.0.2.1`  
`server 2001:db8::1`  
`server time.example.net`  

“noquery” is required to disable MONLIST
Prevent IP Spoofing (network hygiene)

• BCP38 / RFC2827 (ingress filtering) – May, 2000:
  • http://bcp38.info/
  • http://www.ietf.org/rfc/bcp/bcp38.txt
  • http://www.ietf.org/rfc/rfc2827.txt

• BCP84 / RFC3704 (for multihomed) – March, 2004:
  • http://www.ietf.org/rfc/bcp/bcp84.txt
  • http://www.ietf.org/rfc/rfc3704.txt
Securing CDN traffic at CloudFlare
CloudFlare security

CloudFlare leverages the knowledge of a diverse community of websites to power a new type of security service. Online threats range from nuisances like comment spam and excessive bot crawling to malicious attacks like SQL injection and denial of service (DOS) attacks. CloudFlare provides security protection against all of these types of threats and more to keep your website safe.

Automatic learning of new attacks

CloudFlare’s technology automatically detects new attacks that arise against any website on its network. Once CloudFlare identifies that there is a new attack, CloudFlare starts to block the attack for both the particular website and the entire community. This also means the longer you are on CloudFlare, the better the protection becomes. See a customer case study at the CloudFlare blog.
CloudFlare – a global network

Attack traffic is global and hence a global edge is valuable
Anycast Dilutes Attacks

300Gbps of attack traffic
/ 29 locations

= ~10.3Gbps average per location
Hide Origin IPs

• Use separate IPs for HTTP, DNS, SMTP, etc

• Public DNS should route to your EDGE’s public IPs

• Keep actual/origin web device IPs protected
Filter traffic by IP and protocol

- No UDP packets should be able to hit your HTTP server
  - UDP is IP protocol 17 vs. TCP for HTTP is IP protocol 6

- No HTTP packets should be able to hit your SMTP server
  - HTTP is TCP port 80 & 443 vs. SMTP is port 25 & 587
Filter traffic by IP and protocol

Simple Cisco filter configuration example

```
!  
hostname router-www  
!  
interface ethernet0  
  ip access-group 102 in  
!  
access-list 102 permit tcp any host 10.0.0.100 eq 80  
access-list 102 permit tcp any host 10.0.0.100 eq 443  
access-list 102 deny all  
!  
```

Allow only HTTP & HTTPS via TCP protocol to a specific IP
Protect your infrastructure

- Internal switches, routers, and other devices should be locked down from any external access

- All traffic should flow through EDGE devices which handle attacks
  - CloudFlare Web Application Firewall (WAF) service
Build relationships upstream

• Understand what your data center and bandwidth providers do about DDoS

• Know who to call when trouble strikes

• Share your IP/Protocol architecture with them
Communicate about attacks

Enormous DNS DDoS attack originates from anti-DDoS service providers

BIGGEST DDoS ATTACK IN HISTORY hammers Spamhaus
Plucky mail scrubbers battle internet carpet bombers

Technical Details Behind a 400Gbps NTP Amplification DDoS Attack

Published on February 13, 2014 01:00AM by Matthew Prince.
Summary
Summary

• First, make sure you’re not part of the problem ...

• Second, practice good protocol hygiene ...

• Third, implement infrastructure ACLs ...

• Fourth, know your upstreams ...
Questions?

Martin J. Levy, Network Strategy
@mahtin
@cloudflare
http://cloudflare.com/