No Cloud Allowed

Denying Service to DDOS Protection Services

Presented by:
Allison Nixon
Allison.Nixon@integralis.com
Pentesting, Incident Response
PaulDotCom host

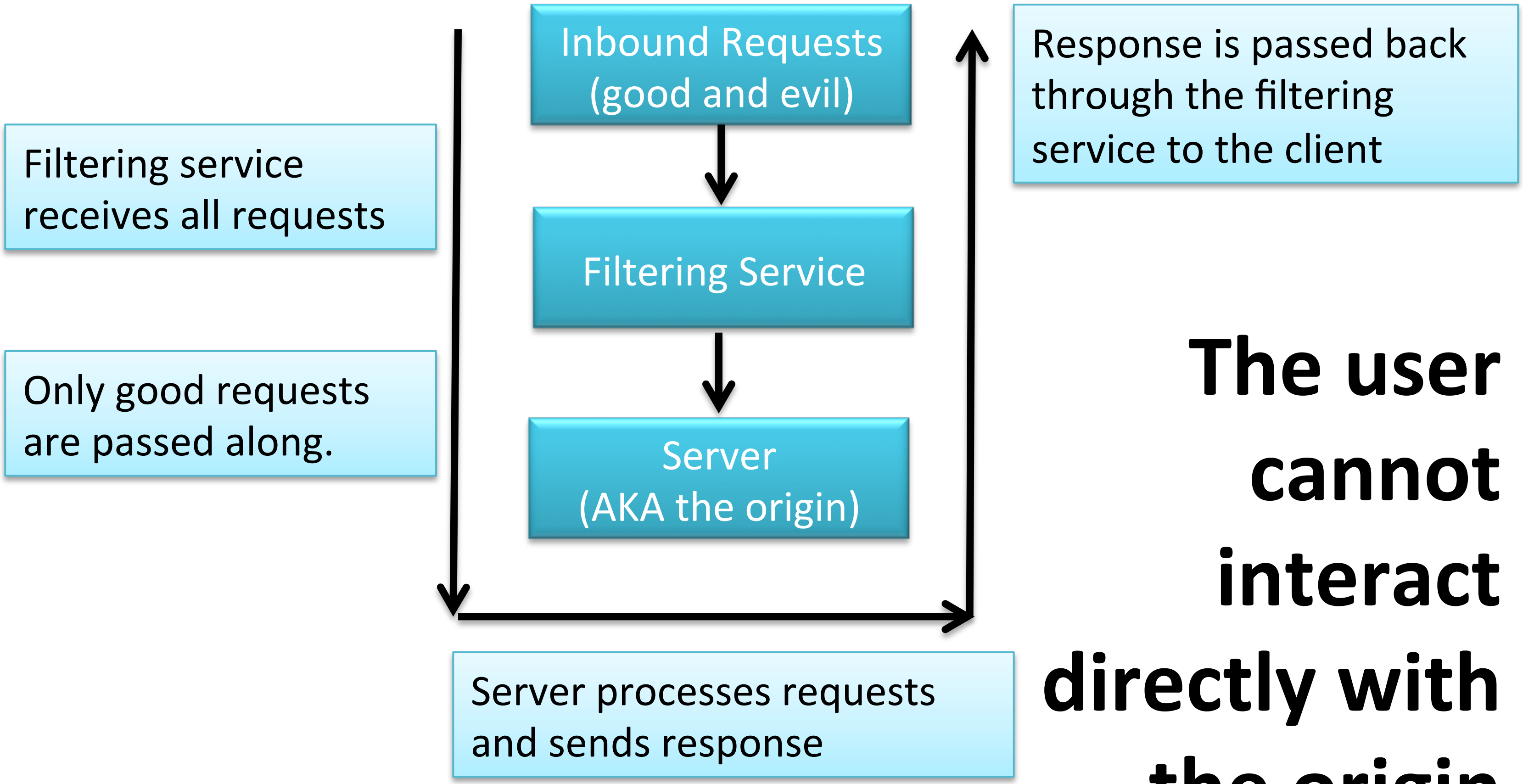
INTEGRALIS

an NTT Communications Group Company

Cloud Based DDOS Protection

- How it works
- Fundamental flaws
- Many ways to find the origin IP
- Mitigating the threat
- Other alternatives

How it Works – Filtering Traffic in Theory



Inbound Requests (good and evil)

Filtering Service

Server (AKA the origin)

Filtering service receives all requests

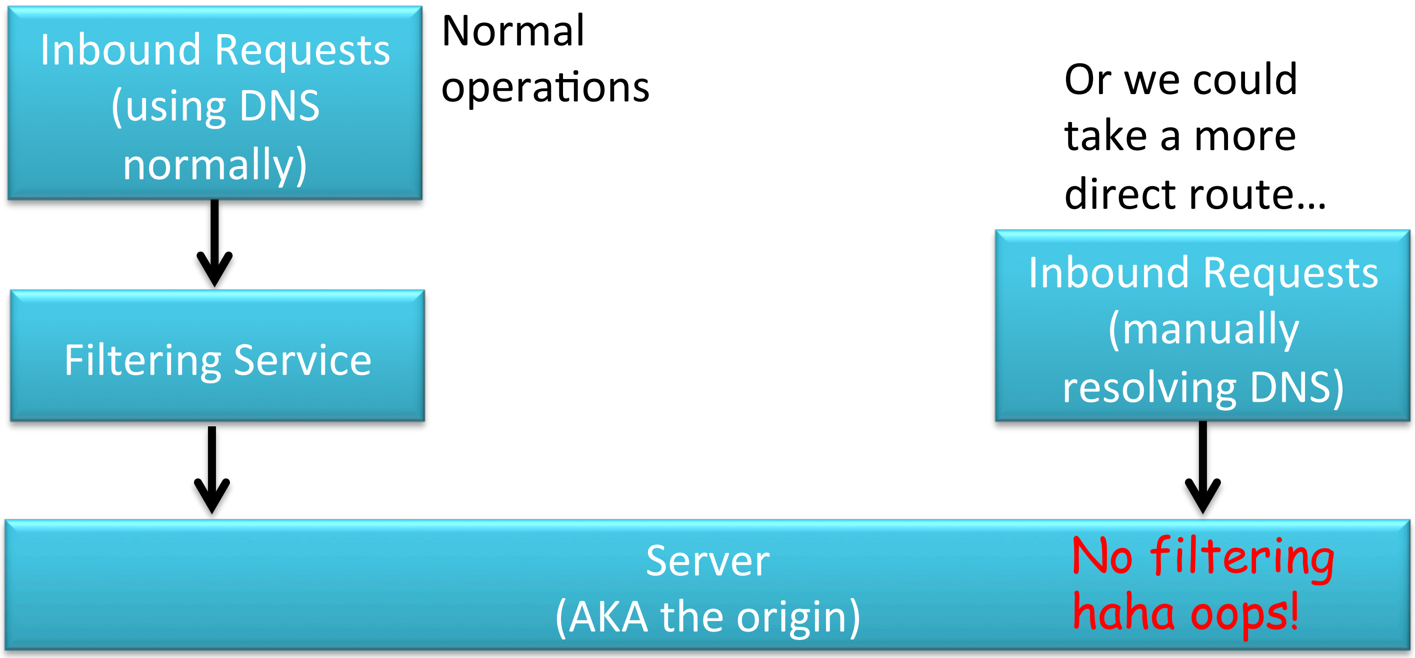
Only good requests are passed along.

Server processes requests and sends response

Response is passed back through the filtering service to the client

The user cannot interact directly with the origin

How it Works – DNS Based Mitigation


Inbound Requests (using DNS normally)
Filtering Service
Inbound Requests (manually resolving DNS)
Server
(AKA the origin)
No filtering
haha oops!

Normal operations

Or we could take a more direct route…

Pointing your DNS to the filter will not block traffic to the origin

DNS resolution is NOT a network access control

The origin IP can be kept secret but this is security by obscurity

All filtering/DDoS blocking can be bypassed if the origin can be found

Fundamental Flaws

Cloud Based DDoS protection bypass

- Fundamental flaws - Mitigations are messy and difficult
- Multiple providers are affected, including the largest ones on the market

Techniques may be effective for other cloud-based filtering services like WAF and e-mail filtering

Fundamental Flaws

Three ways to route traffic: DNS, BGP, inline

Using DNS to reroute traffic

- Clever attackers can send traffic to the origin
- There is low awareness of just how easy it is
- Every provider that uses DNS based mitigation is affected

Providers that use BGP based mitigation or inline filtering are not affected

- BGP is practically inline because IP traffic cannot choose how it is routed

Fundamental Flaws

A server's public facing IP was not intended to be secret information

Many sources of information leakage can reveal the origin.

Once the origin IP is known, all protection is lost

Unmasking an origin is very easy

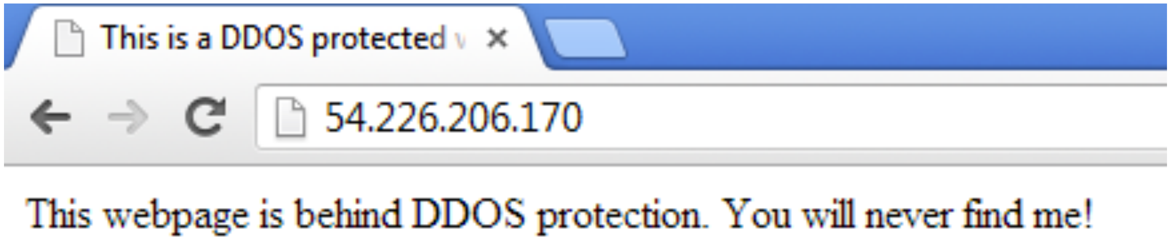
Many ways to find the origin IP

Verifying the origin IP is straightforward

- Manually resolve DNS and view the origin's website directly
- If firewall rules prevent verification, DDoS the origin
  - The provider will show a cached copy of the site if the origin is unreachable

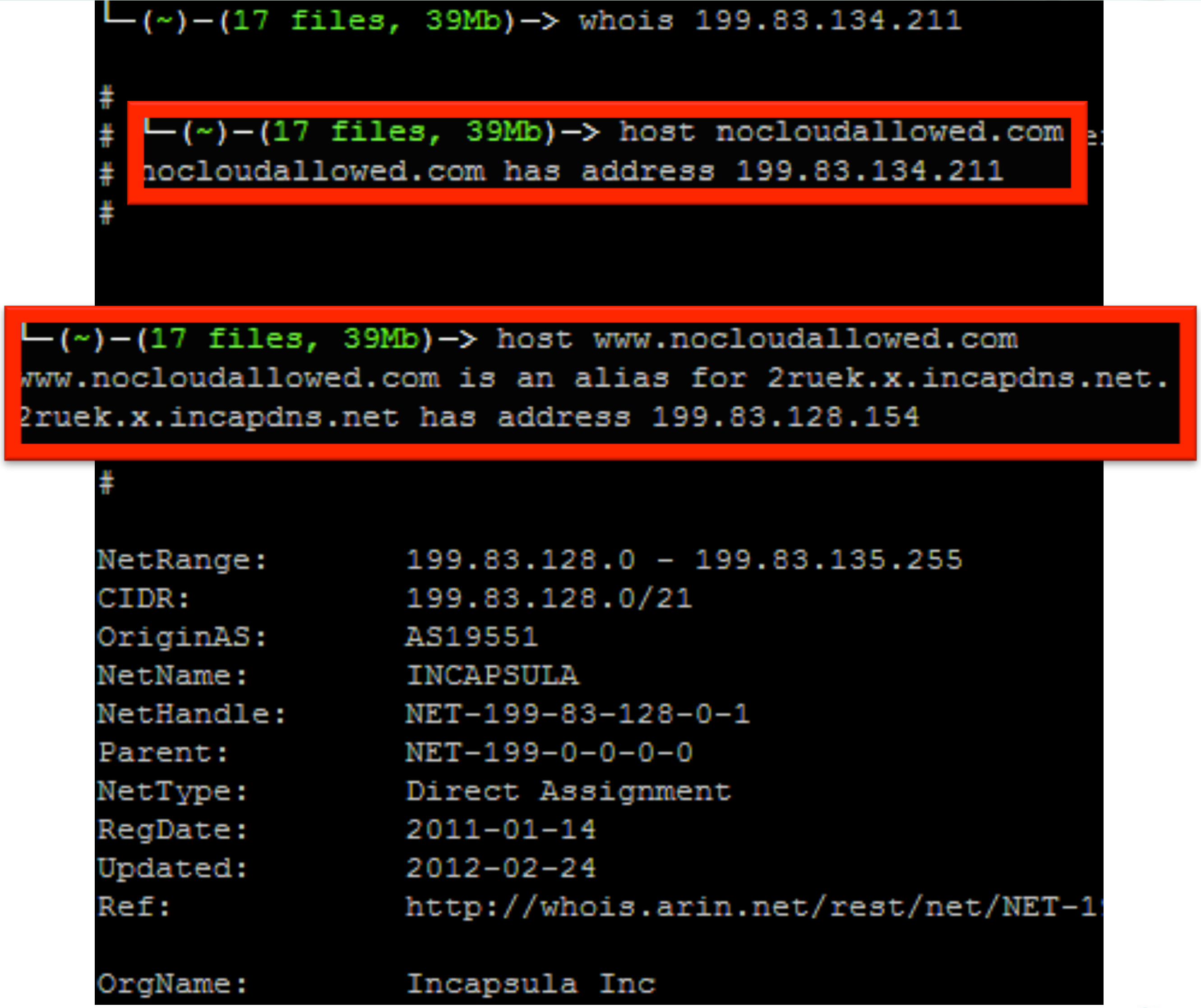
Many ways to find the origin IP

Verifying the origin IP is straightforward



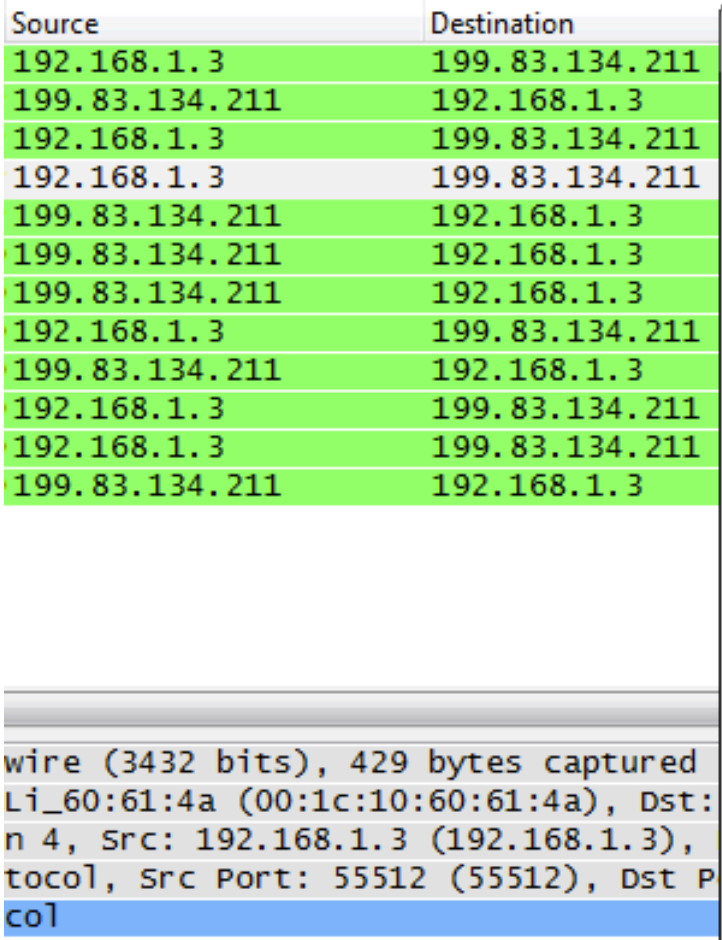
This webpage is behind DDOS protection. You will never find me!

Many ways to find the origin IP



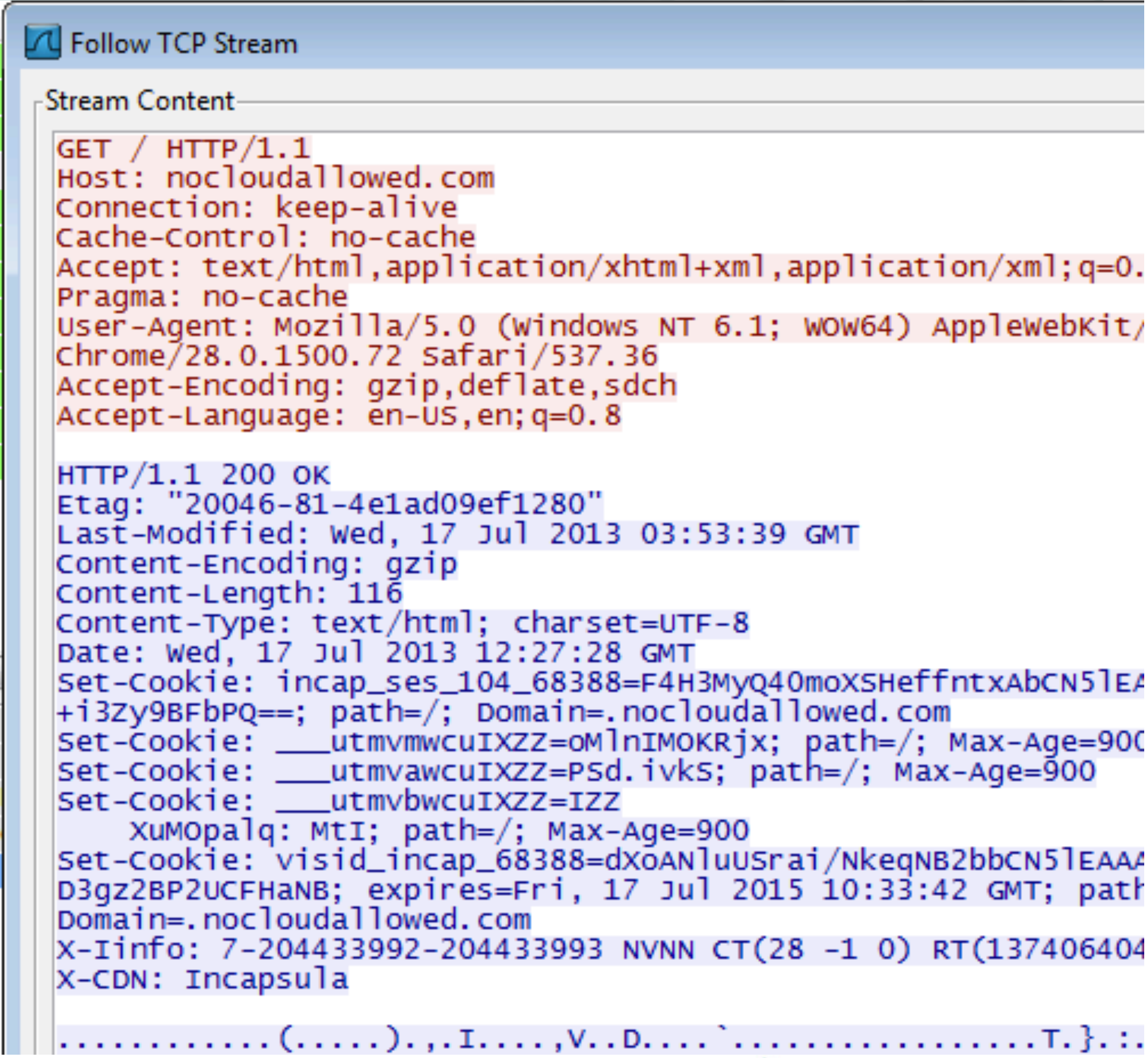
```
└─(~)─(17 files, 39Mb)─> whois 199.83.134.211

#
# └─(~)─(17 files, 39Mb)─> host nocloudallowed.com
# nocloudallowed.com has address 199.83.134.211
#

└─(~)─(17 files, 39Mb)─> host www.nocloudallowed.com
www.nocloudallowed.com is an alias for 2ruek.x.incapdns.net.
2ruek.x.incapdns.net has address 199.83.128.154
#

NetRange:       199.83.128.0 - 199.83.135.255
CIDR:           199.83.128.0/21
OriginAS:       AS19551
NetName:        INCAPSULA
NetHandle:      NET-199-83-128-0-1
Parent:         NET-199-0-0-0-0
NetType:        Direct Assignment
RegDate:        2011-01-14
Updated:        2012-02-24
Ref:            http://whois.arin.net/rest/net/NET-1

OrgName:        Incapsula Inc
```

Many ways to find the origin IP



Source	Destination
192.168.1.3	199.83.134.211
199.83.134.211	192.168.1.3
192.168.1.3	199.83.134.211
192.168.1.3	199.83.134.211
199.83.134.211	192.168.1.3
199.83.134.211	192.168.1.3
199.83.134.211	192.168.1.3
192.168.1.3	199.83.134.211
199.83.134.211	192.168.1.3
192.168.1.3	199.83.134.211
192.168.1.3	199.83.134.211
199.83.134.211	192.168.1.3

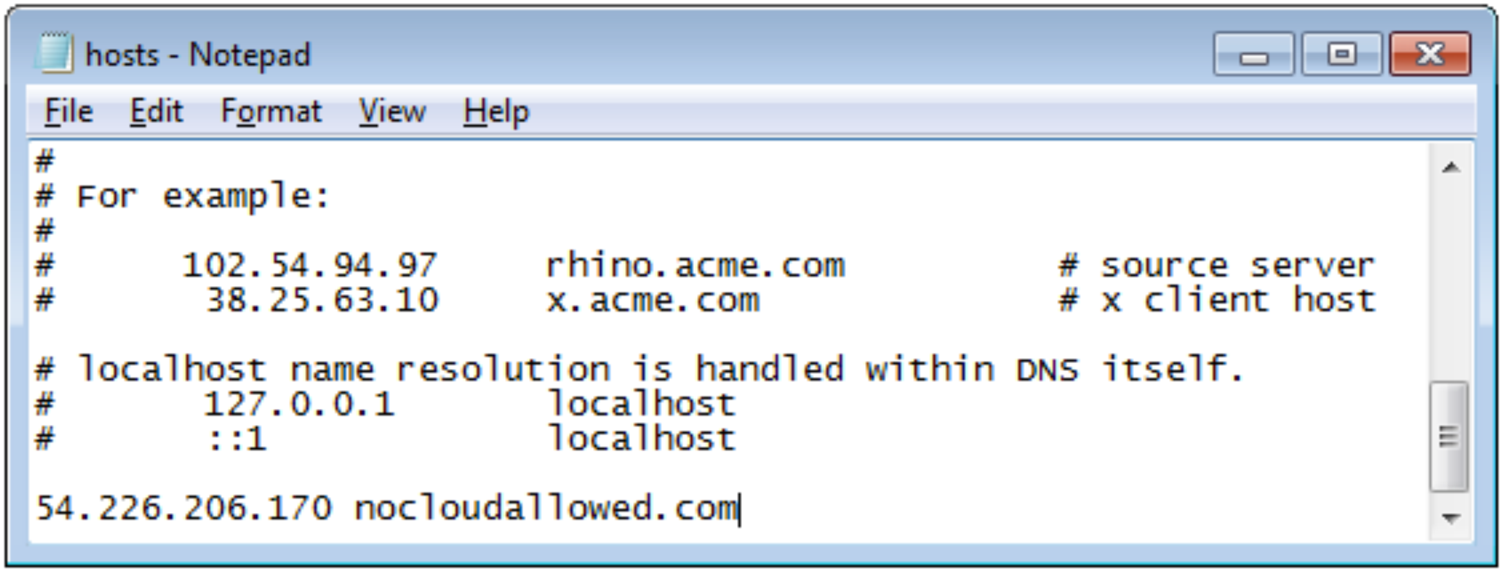
```
wire (3432 bits), 429 bytes captured
Li_60:61:4a (00:1c:10:60:61:4a), Dst:
n 4, Src: 192.168.1.3 (192.168.1.3),
tocol, Src Port: 55512 (55512), Dst P
col
```



```
GET / HTTP/1.1
Host: nocloudallowed.com
Connection: keep-alive
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/
Chrome/28.0.1500.72 Safari/537.36
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
Etag: "20046-81-4e1ad09ef1280"
Last-Modified: Wed, 17 Jul 2013 03:53:39 GMT
Content-Encoding: gzip
Content-Length: 116
Content-Type: text/html; charset=UTF-8
Date: Wed, 17 Jul 2013 12:27:28 GMT
Set-Cookie: incap_ses_104_68388=F4H3MyQ40moXSHeffntxAbCN5lEA
+i3Zy9BFbPQ==; path=/; Domain=.nocloudallowed.com
Set-Cookie: ___utmvmwcuIXZZ=oMlnIMOKRjx; path=/; Max-Age=900
Set-Cookie: ___utmvawcuIXZZ=PSd.ivkS; path=/; Max-Age=900
Set-Cookie: ___utmvbwcuIXZZ=IZZ
    XuMOpalq: MtI; path=/; Max-Age=900
Set-Cookie: visid_incap_68388=dXoANluUSrai/NkeqNB2bbCN5lEAA
D3gz2BP2UCFHaNB; expires=Fri, 17 Jul 2015 10:33:42 GMT; path
Domain=.nocloudallowed.com
X-Iinfo: 7-204433992-204433993 NVNN CT(28 -1 0) RT(137406404
X-CDN: Incapsula

............(.....).,.I....,V..D....`................T.}.:.
```

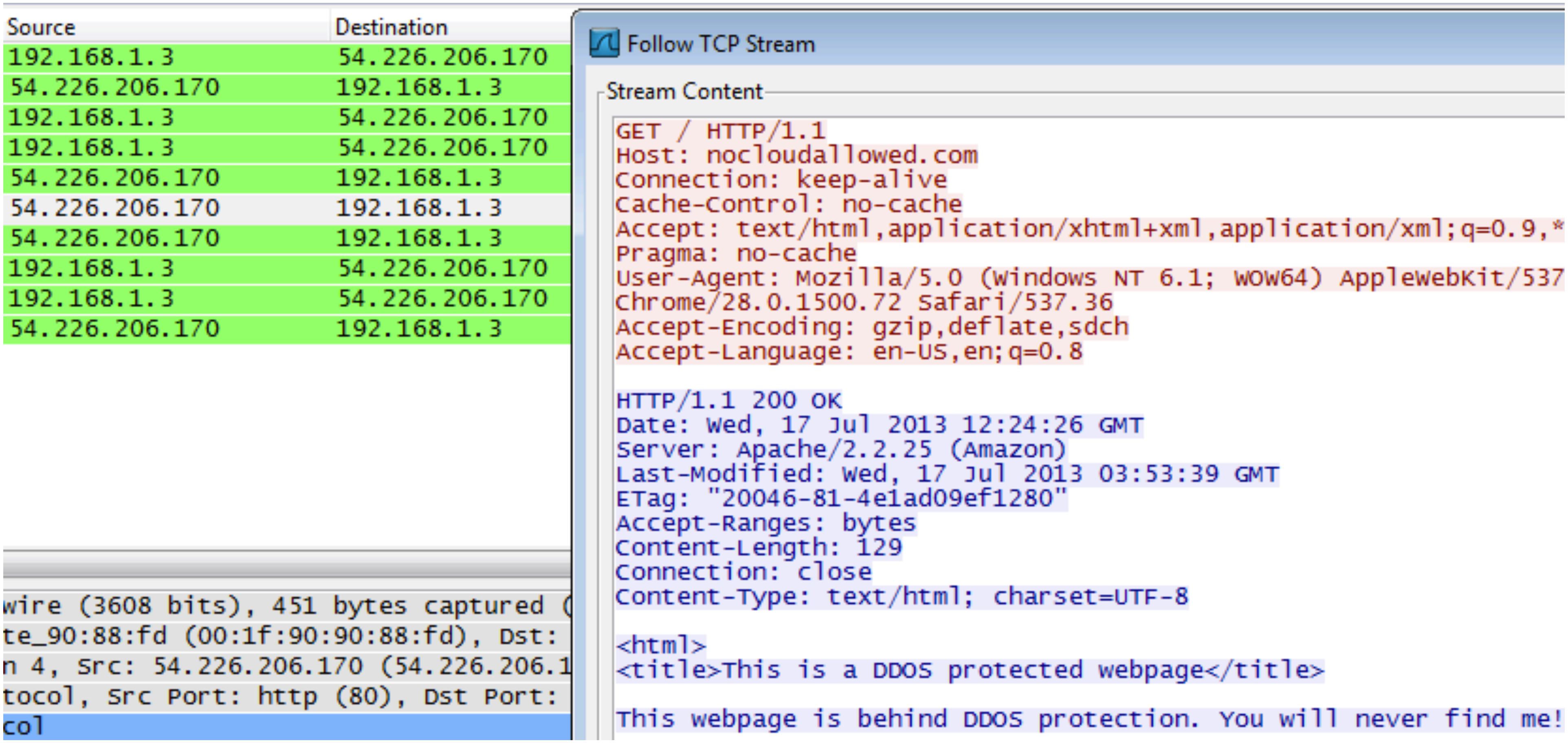
Many ways to find the origin IP

Verifying the origin IP is straightforward



```
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

54.226.206.170 nocloudallowed.com
```

Many ways to find the origin IP



Source	Destination
192.168.1.3	54.226.206.170
54.226.206.170	192.168.1.3
192.168.1.3	54.226.206.170
192.168.1.3	54.226.206.170
54.226.206.170	192.168.1.3
54.226.206.170	192.168.1.3
54.226.206.170	192.168.1.3
192.168.1.3	54.226.206.170
192.168.1.3	54.226.206.170
54.226.206.170	192.168.1.3

```
wire (3608 bits), 451 bytes captured (
te_90:88:fd (00:1f:90:90:88:fd), Dst:
n 4, Src: 54.226.206.170 (54.226.206.1
tocol, Src Port: http (80), Dst Port:
col
```

```
GET / HTTP/1.1
Host: nocloudallowed.com
Connection: keep-alive
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537
Chrome/28.0.1500.72 Safari/537.36
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
Date: Wed, 17 Jul 2013 12:24:26 GMT
Server: Apache/2.2.25 (Amazon)
Last-Modified: Wed, 17 Jul 2013 03:53:39 GMT
ETag: "20046-81-4e1ad09ef1280"
Accept-Ranges: bytes
Content-Length: 129
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
<title>This is a DDOS protected webpage</title>

This webpage is behind DDOS protection. You will never find me!
```

Many ways to find the origin IP - DNS

Related DNS records

- www.victim.com points to a DDoS protection provider’s range, but ftp.victim.com points to the origin
- www.victim2013event.com may point to the origin. Check all domains owned by your target

Historical DNS records

- If the origin IP was not changed after protection is set up, historical DNS services exist that could have recorded the origin IP

Many ways to find the origin IP - Connections

Outbound connections to an attacker controlled server

- DDoS protection services act as HTTP reverse proxies, but they do not proxy outbound connections
- Application specific features like “avatar upload” on forums

Outbound e-mail headers

- “I forgot my password”
- “I wish to subscribe to your newsletter”

Many ways to find the origin IP - Leaks

Server specific information leakage

- HTTP authorization sometimes leak origin IP

Application specific information leakage

- Overly helpful error messages
- Exposed config files

Many ways to find the origin IP - Providers

DMCA complaints

- Submit bogus DMCA complaints to obtain the origin IP of Cloudflare customers*

Other types of abuse complaints

- Depends on the policies of the DDoS protection provider

Exceeding capacity

- DDoSing with a large enough attack can apparently drop the customer into bypass mode, especially for cheap/free accounts**

* http://blog.cloudflare.com/thoughts-on-abuse

** link to a google cached version of a malicious "Cloudflare dropping" service. Not personally tested by me

Many ways to find the origin IP - Other

As of yet undiscovered methods to discover the origin IP

- Not much serious research has been done in getting a server to divulge its public facing IP, because this is generally not a security issue
- If more research is done, more exploits may emerge

Target specific information leakage

- Information is not considered sensitive so may be carelessly left around, can be found manually

Many ways to find the origin IP - Scanner

NoCloudAllowed.com ☹

- Scans the entire Internet for servers that look like the protected website
- Same method as manual origin verification, but against every IP in an arbitrary range
- Unmasks the origin even in the absence of information leakage
- Obscurity is no more

Mitigating the Threat

Non-standard configurations to prevent unmasking

- Block traffic from outside the provider’s range

Mitigation techniques may harm availability

- Blocking outside requests can backfire if the provider must go into bypass mode or the provider sends traffic from new ranges

Security non-issues become security issues

- The public facing IP of a server is generally not considered sensitive data, apps are not designed to conceal this

Mitigating the Threat

Inspect all apps for outbound connections

Outbound mail must obscure the source

Check error messages for IP leakage

Remove all DNS records pointing to the origin

Security by obscurity

Fix IP leakage issues specific to your setup

Attackers bypass your protections every time they find your IP

Change your IP every time it is leaked

Fix problems caused by changing your server's IP

Other Alternatives

Ask your provider if they use DNS or BGP for rerouting traffic

- If BGP, they will require that you own a /24 and BGP capable router and a few other things. Direct to origin attacks won't work while it's on
- If DNS only, get ready for some hide and seek

If you use an inline appliance, it cannot be bypassed using these tricks

Other Alternatives

So you want to use DNS based mitigation…

- Play hide and seek
- Solve new problems

Inline or BGP based mitigations

- At least you don’t need to play hide and seek with your IT infrastructure

Vender’s responses

“It’s a known issue”

Thank you

NoCloudAllowed.com

Allison Nixon
Integralis Inc.
allison.nixon@integralis.com

Special thanks to Chris Camejo, Brandon Levene