CISCO
SECURE

Combating Disinformation in DNS and Beyond

Blake Anderson, PhD
blake.anderson@cisco.com

FloCon - January 2023

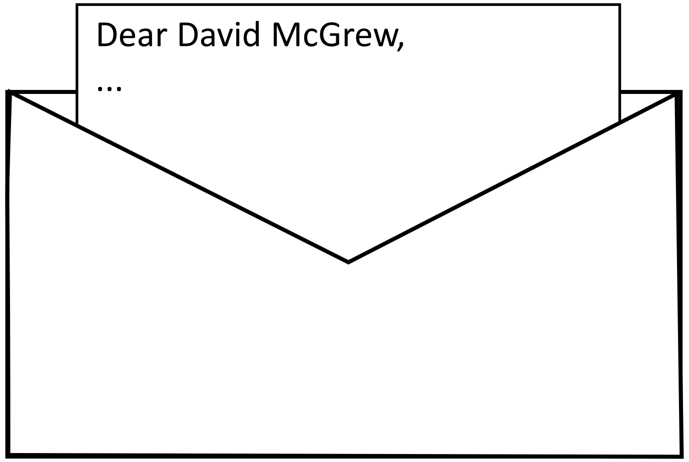
CISCO The bridge to possible

Overview

- Domain fronting highlights
  - MITRE ATT&CK: T1090.004
  - Abuses encryption standards and CDN mechanics
  - Misleads security tools about the server's identity
- Domain fronting's current use
  - Malware authors and attack tools
  - Privacy-focused tools
- Network Defenders should
  - Reevaluate how current network IoC's are used in production

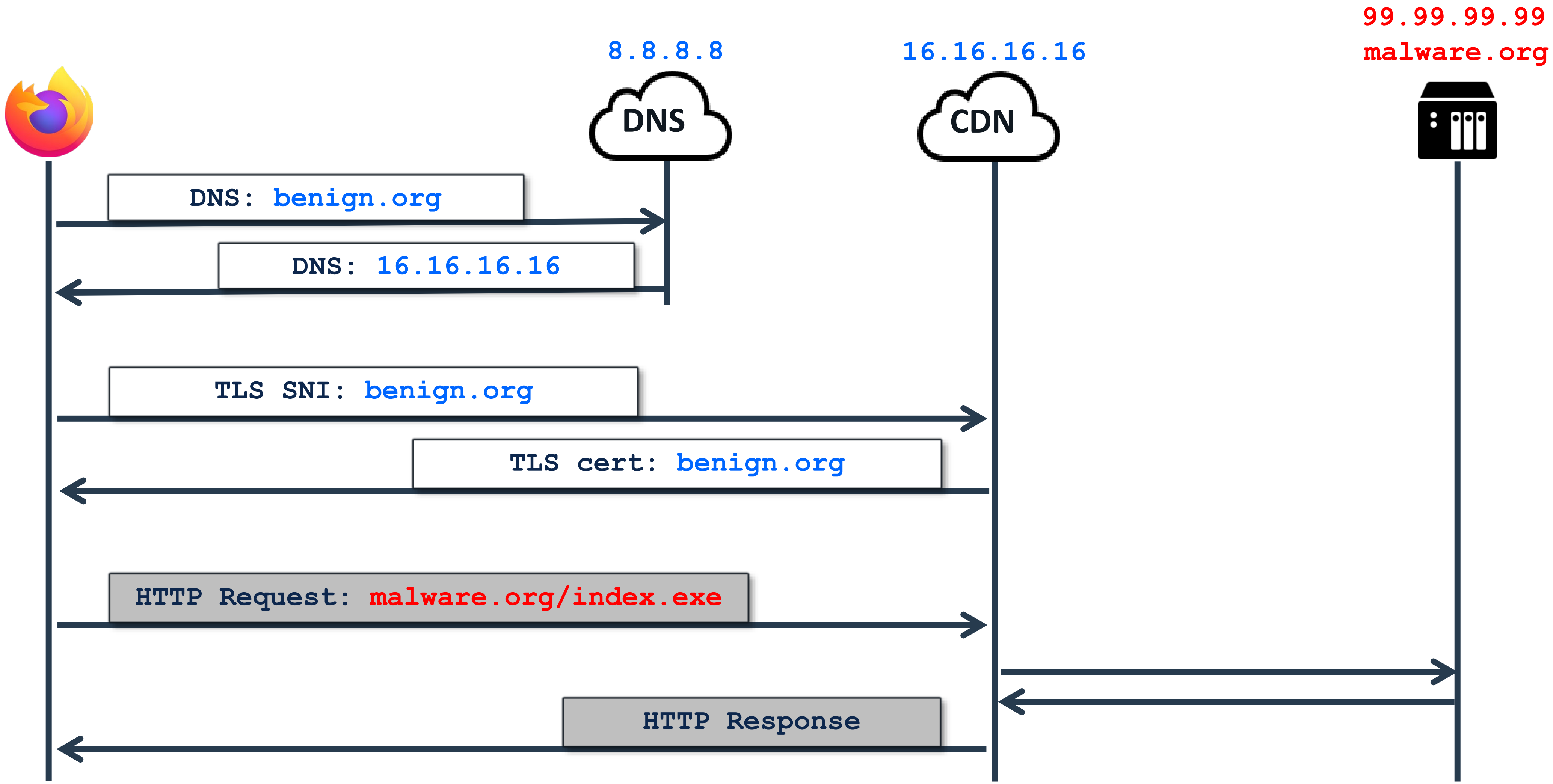
Domain Fronting Analogy

ATTN: Blake Anderson
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA

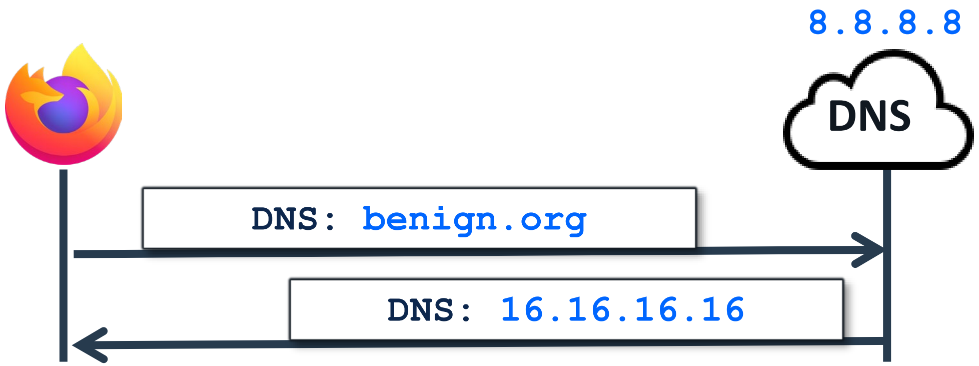


Dear David McGrew,
...

Domain Fronting

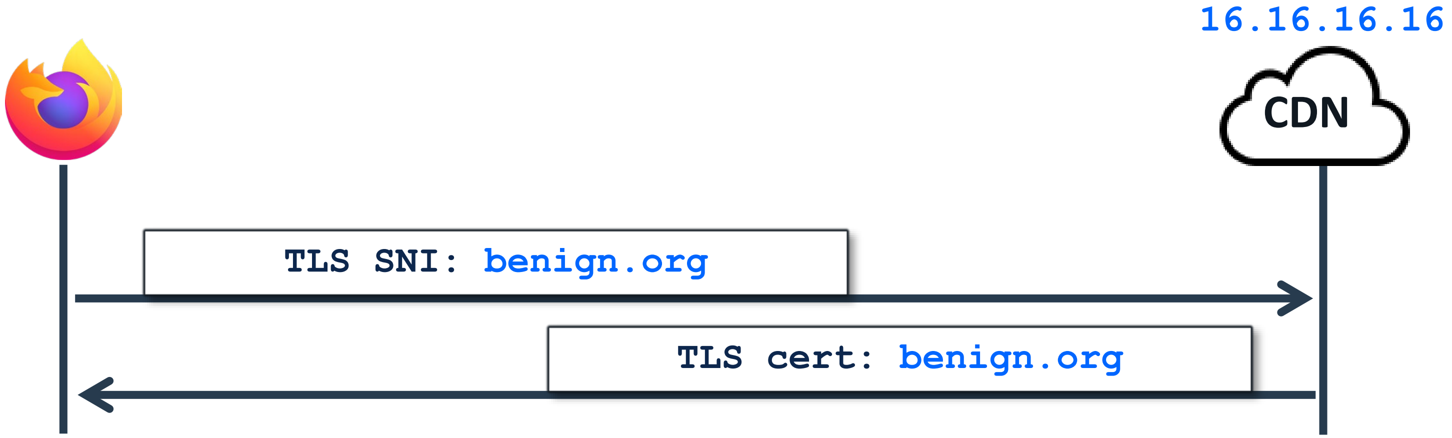


Domain Fronting Observables (DNS)



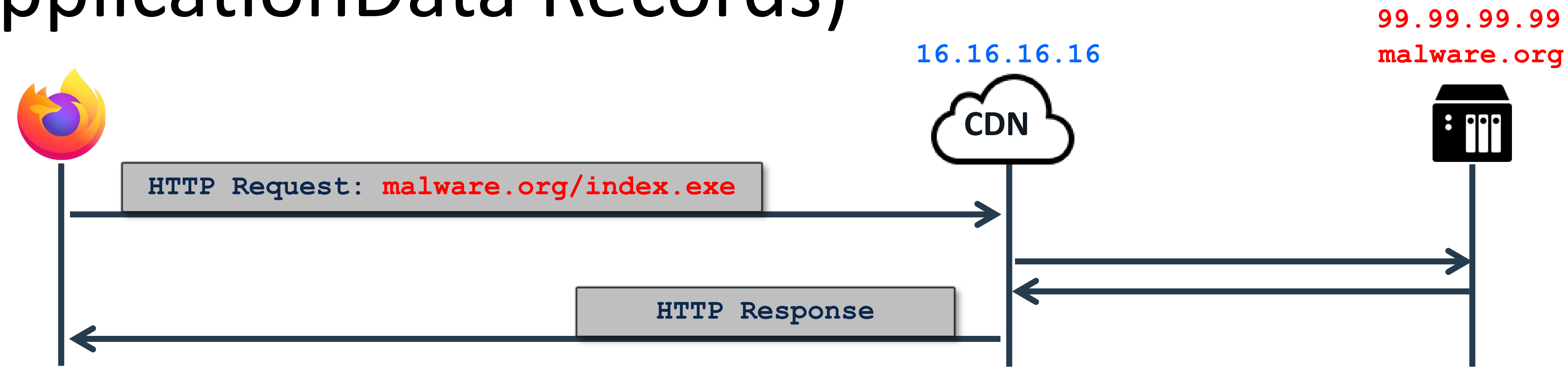
Observables	Value	Notes
DNS Requested Domain	benign.org	A benign, prevalent domain
DNS Response, IP Address	16.16.16.16	The CDN’s IP address
DNS Response, CNAME	j.sni.global.fastly.net	Supports domain fronting?
DNS Server’s IP address	8.8.8.8	Potentially unsanctioned

Domain Fronting Observables (TLS Handshake)



Observables	Value	Notes
TLS server_name	benign.org	A benign, prevalent domain
TLS Fingerprint	tls/1/(0303)(1303)[(0000)...]	Could indicate evasive software
TLS Certificate	benign.org	Legitimate certificate
Destination IP Address	16.16.16.16	The CDN’s IP address

Domain Fronting Observables (TLS ApplicationData Records)



Observables	Value	Notes
Destination IP Address	16.16.16.16	The CDN’s IP address

Non-Observables	Value	Notes
HTTP Host	(Encrypted) malware.org	Would need TLS decrypt
Origin IP Address	99.99.99.99	Only available to the CDN

Measurement

Mining DNS CNAME Records

```
/:~$ host -v www.example.com

;; QUESTION SECTION:
;www.example.com.        IN     A

;; ANSWER SECTION:
www.example.com.          0      IN     CNAME ghs.googlehosted.com.
ghs.googlehosted.com.     0      IN     A     142.251.40.83
```

- Collect domain names, IP addresses, CDN hostnames

Collecting Data

- Custom PySpark Scanning Infrastructure
  - Rewrites DNS responses for ground truth on IP addresses
  - Collect:
    - TLS certificates
    - HTTP response headers
    - HTTP response content
- For pairs of domains using the same top-level CDN hostname:

```
#               scan_host(dst_ip,    http_host,       tls_server_name)
ret_baseline  = scan_host(target_ip, target_domain,   target_domain)
ret_front     = scan_host(front_ip,  target_domain,   front_domain)
ret_all_front = scan_host(front_ip,  front_domain,    front_domain)
ret_fake      = scan_host(target_ip, target_domain,   front_domain)
ret_garbage   = scan_host(target_ip, target_domain,   'aaaaaaaa')
ret_no_sni    = scan_host(target_ip, target_domain)
```

Scan Results

CDN / Hostname	% Fronting Support
`*.googlehosted.com.`	100.00%
`*.stackpathcdn.com.`	100.00%
`*.wixdns.net.`	99.83%
`*.impervadns.net.`	99.41%
`*.incapdns.net.`	99.31%
`*.fastly.net.`	56.21%
`*.akamaiedge.net.`	2.77%
`*.amazonaws.com.`	1.25%
`*.cloudapp.net. (MSFT)`	0.67%
`*.azure.com.`	0.62%
`*.cloudflare.net.`	0.00%
`*.herokudns.com.`	0.00%

Other Popular CDNs with Majority Support: Bunny CDN, Netlify, CDN77, KeyCDN, Limelight, ...

Frontable Domains

Domain	Umbrella Rank	CDN
ctldl.windowsupdate.com	14	StackPath
inappcheck.itunes.apple.com	270	Alibaba
download.windowsupdate.com	593	StackPath
www.amazon.com	655	Fastly
trc.taboola.com	701	Fastly
cdn.flashtalking.com	1,058	StackPath
au.download.windowsupdate.com	1,291	StackPath
pips.taboola.com	1,542	Fastly
pi.ispot.tv	2,222	Fastly
zem.outbrainimg.com	2,391	Fastly

Umbrella top-1m.csv

Discussion

General Recommendations

- The TLS **server_name** and **certificate** should not be implicitly trusted.
  - Need to correlate with other data features

- Supporting Measurement:
  - Track destinations/hosting providers/processes

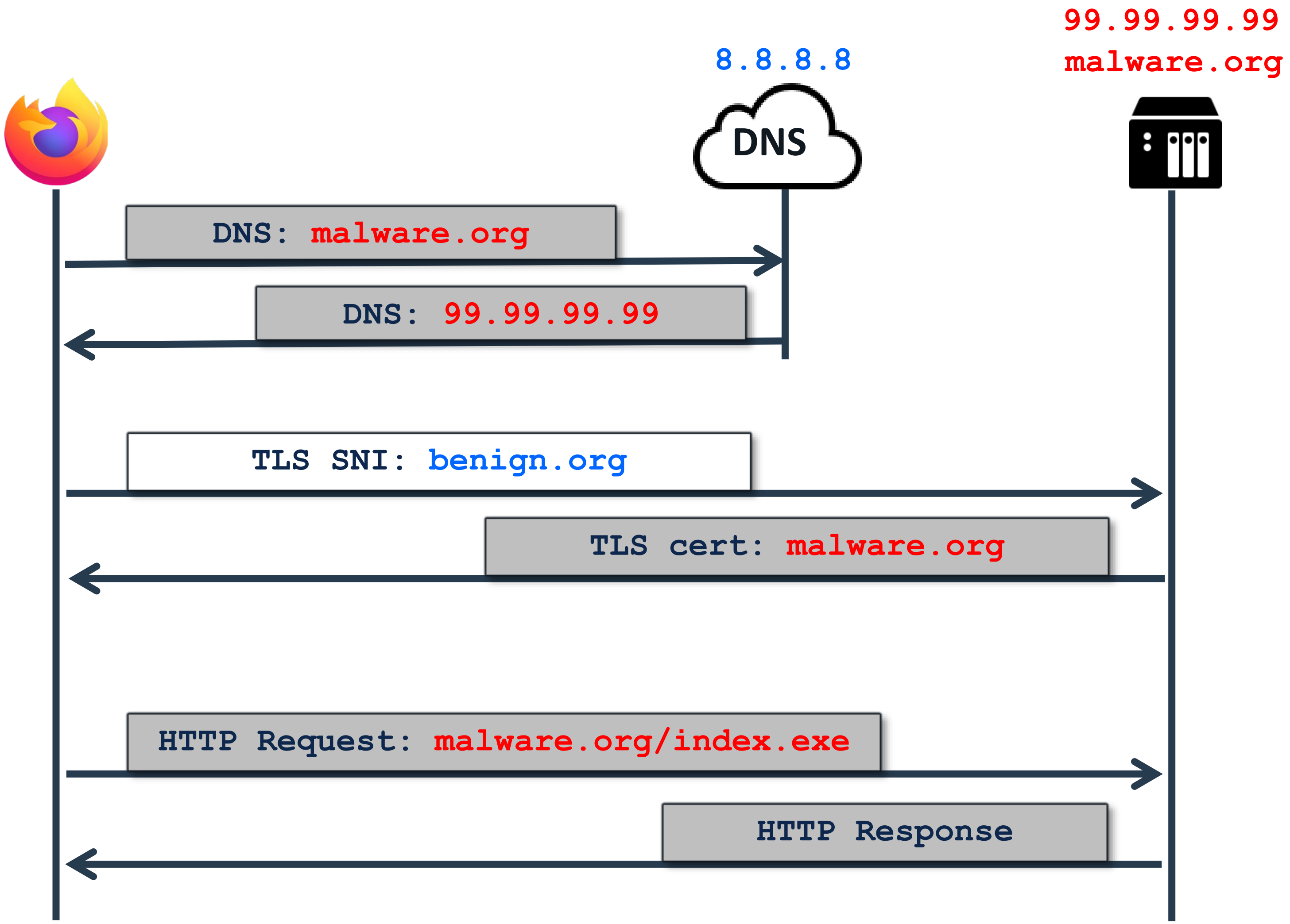
Potential Data Features

- IP subnets with substantial support
  - **151.101.0.0/16**
- Canonical names likely to support domain fronting
  - e.g., **`j.sni.global.fastly.net.`**
- Process names/hashes that support domain fronting
  - e.g., **psiphon**, **cyberghost**, **curl –H “Host: ”**
- Domains commonly used to front
  - e.g., **b-cdn.net** (psiphon)

SECURE

Related Misinformation Techniques

Domain Faking



8.8.8.8

99.99.99.99
malware.org

DNS

DNS: malware.org

DNS: 99.99.99.99

TLS SNI: benign.org

TLS cert: malware.org

HTTP Request: malware.org/index.exe

HTTP Response

Domainless and Wildcard Fronting

- Domainless Fronting
  - Omit the server_name extension
  - Set the server_name extension to “”
- Wildcard Fronting
  - Leverage overly broad certificates
  - e.g., *.cloudfront.net, *.s3.amazonaws.com, *.appspot.com

Scan Results

CDN / Hostname	% Faking Support	% Domainless Support
*.googlehosted.com.	100.00%	0.05%
*.wixdns.net.	99.83%	0.00%
*.fastly.net.	99.58%	99.34%
*.stackpathcdn.com.	99.53%	98.72%
*.impervadns.net.	98.61%	95.76%
*.cloudapp.net. (MSFT)	98.09%	98.06%
*.incapdns.net.	98.07%	95.86%
*.amazonaws.com.	95.70%	95.52%
*.azure.com.	93.04%	94.45%
*.akamaiedge.net.	52.11%	51.04%
*.cloudflare.net.	0.51%	16.77%
*.herokudns.com.	0.00%	0.00%