Domain Fronting FTW!

Why you could and should use domain fronting on engagements

Matt George | Analyst | phia, LLC
SANS Hackfest 2018 | November 12th – 13th
Who Am I?

- **Currently:**
  - Federal contractor, threat hunting and threat detection analytics
  - Research and emulate threats and techniques for customers
  - Aspiring pen tester
  - SANS 504 Mentor/Advisory Board
  - NoVA Hackers

- **Formerly:**
  - Satellite terminal operator, firewall tech support, network engineer
  - IT systems engineer/administrator
  - Enterprise security analyst/defender
Objective: Demystify the technique, discuss issues

Background
- CDNs/CSPs

Domain Fronting
- Technical details
- Use cases
- Identification
- History
- In the News
- Risks
- How/When to use it
- Future
Content Delivery Networks

- Level set on CDNs/CSPs
  - Crucial to understanding Domain Fronting
- Meets business needs:
  - Localized delivery of content (decentralized)
  - Scalability
  - Resilience
Content Delivery Networks
Content Delivery Networks

- Get MOAR memes/cat pics faster!
Content Delivery Networks

- **CDNs:**
  - Get content to the user faster and in larger quantities
  - Images, videos, ads, scripts, web elements etc.
  - Coalesces the bits in the browser

- **Performance, load balancing, caching**

- **Manipulates “normal” DNS behavior, pointing clients to provider edge nodes**
  - “DNS Gerrymandering”
  - Leads to other issues

- **Essentially inserts a Man-in-the-Middle between client and server**
  - Introduces risk
What is Domain Fronting?

- An undocumented feature of Content Delivery Networks and Cloud Service Providers that allows clients to proxy web traffic through them covertly
- Uses different destinations at different layers
- Combined with encryption = dangerous
- Abuses the way CDNs/CSPs redirect traffic
- A topic of much controversy
- Introduces significant risk for organizational networks
What is Domain Fronting?

- Seminal paper on the topic:
  - [Blocking-resistant Communication Through Domain Fronting](#)
- Several good demos/articles (at the end)
- [MITRE ATT&CK](#)
- [APT 29](#)
What is Domain Fronting?

Web Clients → CDN Edge
- Node1
- Node2
- Node3
- Node4 → CDN Hosting
  - www.good.com
  - www.nothingevil.com
  - www.benign.com
  - www.toteslegit.com
  - www.totesevil.com → Hosted Customers
Fun with Headers – What Routers See

**IP HEADER**
- SOURCE IP ADDRESS: 1.2.3.4
- DESTINATION IP ADDRESS: 5.6.7.8

**TCP HEADER**
- `<FIELDS>`

**TLS CLIENT HELLO**
- SERVER NAME INDICATION: www.totallysafe.com
- `<ENCRYPTED HTTP DATA>`
Fun with Headers – What Servers & Clients See

IP HEADER
- SOURCE IP ADDRESS: 1.2.3.4
- DESTINATION IP ADDRESS: 5.6.7.8

TCP HEADER
- <FIELDS>

TLS CLIENT HELLO
- SERVER NAME INDICATION: www.totallysafe.com

HTTP
- HOST HEADER: www.totallysafe.com

MATCH!
Fun with Headers – What Servers & Clients See

**IP HEADER**
- **SOURCE IP ADDRESS**: 1.2.3.4
- **DESTINATION IP ADDRESS**: 5.6.7.8

**TCP HEADER**
- `<FIELDS>`

**TLS CLIENT HELLO**
- **SERVER NAME INDICATION**: www.totallysafe.com

**HTTP**
- **HOST HEADER**: www.evil.com

*MISMATCH!*
Co-location on service provider’s network
  • The “fronted” domain must exist on the provider’s network
  • Attack machine with listener
  • Alternatively, a bridge/proxy

Browser/script/tool that allows for SNI/HTTP Host Header manipulation

Little to no coding required
  • Cobalt Strike
  • PowerShell Empire
  • Possible:
    o Metasploit
    o Python
    o PowerShell
Use Cases

- Political dissidents, reporters, etc. in heavily censored nations
  - Circumvention of censorship, anti-privacy/anti-free speech controls

- Messaging:
  - Open Whisper apps (WhatsApp, Signal)
  - Telegram

- Proxy networks:
  - Tor (via Meek), Psiphon, Lantern, etc.

- Bad guys exploit this behavior to bypass controls
  - Command and Control, egress, data exfiltration
  - Web proxies, IDS, reputation and blacklist filtering
  - APT29/Cozy Bear/The Dukes (2015)

- And you!
Identification

- **TLS Proxy**
  - Almost nobody does it
  - May or may not be feasible

- **Standard C2/Exfiltration detections in cloud-based traffic:**
  - Block the service provider (Ha!)
  - Internet whitelisting
  - Detect beacons, high producer-to-consumer ratios, long-running, high-volume otherwise “weird” connections
  - Cross-reference, test “frontable” domain lists with web proxy logs/flow data
  - Find other ways to fingerprint services (like TLS cipher list signatures)

- **Standard host-based detections/controls**
  - Application whitelisting
  - CLI logging, shell history, etc.
Fronting History (1)

- 2012: Bryce Boe blog post proves that SNI and HTTP need not agree
- 2014: Meek plugin for Tor uses “Domain Fronting”
- 2015: Documented in a white paper
- 2015: APT29 used in large scale breach
- 2016: Fireeye/Mandiant @ShmooCon and @DerbyCon 2016 reported on APT 29’s use during a 2015 breach
- 2016: Open Whisper announces fronting support using Google, Amazon CloudFront, S3, Azure, Cloudflare, Fastly and Akamai
January 2017: Optiv researchers blogged about fronting using Cobalt Strike

February 2017: Raphael Mudge demos fronting using Cobalt Strike via Malleable C2

April 2018: Google kills fronting on App Engine

April 2018: Amazon kills fronting on CloudFront

May 2018: Privacy advocates petition Google and Amazon to allow Domain Fronting

May 2018: Amazon informs Open Whisper that they are in violation of AWS Service Terms and threatens to suspend the account
“Google kills off domain fronting – and so secure comms just got tougher”  
– April 2018

“Amazon blocks domain fronting, threatens to shut down Signal’s account”  
– May 2018

“Domain fronting has a dwindling future” – July 2018

“Digital Rights Groups Ask Congress for Help as Russia Ramps up Its War on Telegram” – May 2018

“Amazon Bends the Knee to Autocrats, Threatens to Cut Off Signal for Using Anti-Censorship Technique” – May 2018

“Lawmakers call on Amazon and Google to reconsider ban on domain fronting” – July 2018
The Risks

- Clients:
  - It’s illegal in some cases

- Defenders:
  - Perimeter network tools have no clue where the traffic is actually going
  - Risk acceptance by trusting the provider

- Service Providers:
  - Complicit in unintentional web proxy-like behavior
  - Liability

- Black hats/penetration testers:
  - Winning!
To Fix or Not to Fix?

- **Do nothing:**
  - Good for the innocent, bad for the ignorant

- **Organizations/enterprises:**
  - Poses a real security risk

- **Service Providers:**
  - The immediate power to change Fronting
  - Disallow SNI/HTTP Host Header mismatches
  - Shut down bridges

- **IETF:**
  - Update TLS RFC to move the HTTP Host Header outside the encrypted payload
  - Remove the HTTP Host Header (replace with the SNI field value)
  - TLS 1.3 is moving in the opposite direction
When To Use It?

- Use maturity as your guide
- The height of stealth:
  - Use only as required
  - Don’t front unless you need to
- May not be a critical finding
  - Not a lot they can do about it
  - Still raises awareness
Why Use It?

- To accurately model the threats to your clients
- To draw more attention to the issue
- If the issue arises in more places, something will happen (eventually)
The Future of Fronting

- Probably will not last forever
- Eventually all respectable service providers will kill it
- A step towards a 100% attributable Internet
  - Scary!
- People will find other ways around controls
  - Censors will fight those too
- RFCs will continue to favor privacy
  - TLS 1.3 moves everything after the “Hello” messages into the encrypted payload
  - Encrypted SNI coming soon (already implemented in BoringSSL)
Wrap-Up

- **Plan of Action:**
  - Everyone: Learn it (risks vs. costs)
  - Educate others
- **Formulate a strategy and implement**
  - Defenders: Detect it
  - Pen Testers: Use it
- **Voice your opinion**
Sources/Further Reading

- Bryce Boe blog
- Tor Meek documentation
- Vincent Yiu Write-up
- Beau Bullock, Ralph May demo (Tradecraft Security Weekly)
- CyberArk Write-up
- Raphael Mudge/Cobalt Strike Write-up
- Optiv blog post
- Fireeye/Mandiant blog
- Fireeye/Mandiant ShmooCon Talk
- Mitre ATT&CK
- IETF TLS 1.3
- IETF ESNI Draft
- Signal blog post
Thank you!

Matt George
@sircosec | george.m.s@outlook.com | www.sircosec.com