black hat ASIA 2021
May 6-7, 2021
BRIEFINGS

Domain Borrowing: Catch My C2 Traffic If You Can

Tianze Ding / Junyu Zhou

Who are we?

Junyu Zhou @md5_salt

Web Security Researcher & Pentester

Defcon / ZeroNights / HITB speaker

Tencent 腾讯

Tianze Ding

Web Security / Red Team

Found multiple vulnerabilities in Microsoft and Safari

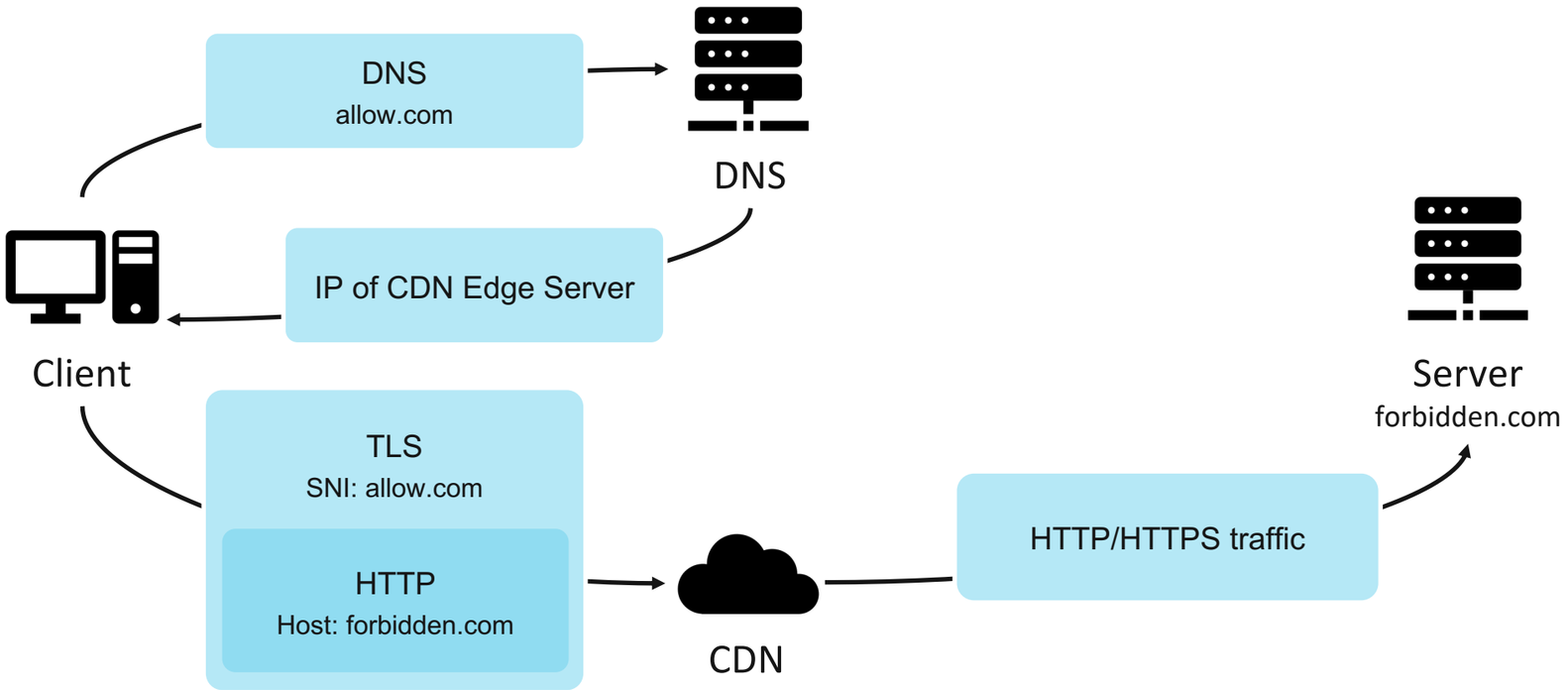
腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

Outline

- Background & Previous Work
  - Domain Fronting
  - Domain Hiding with TLS1.3 and ESNI
- Domain Borrowing
  - The HTTPS CDN workflow
  - Borrow arbitrary domain
  - Borrow valid HTTPS certificates
- Detection & Mitigation
- Demo: Bypass Palo Alto Firewall

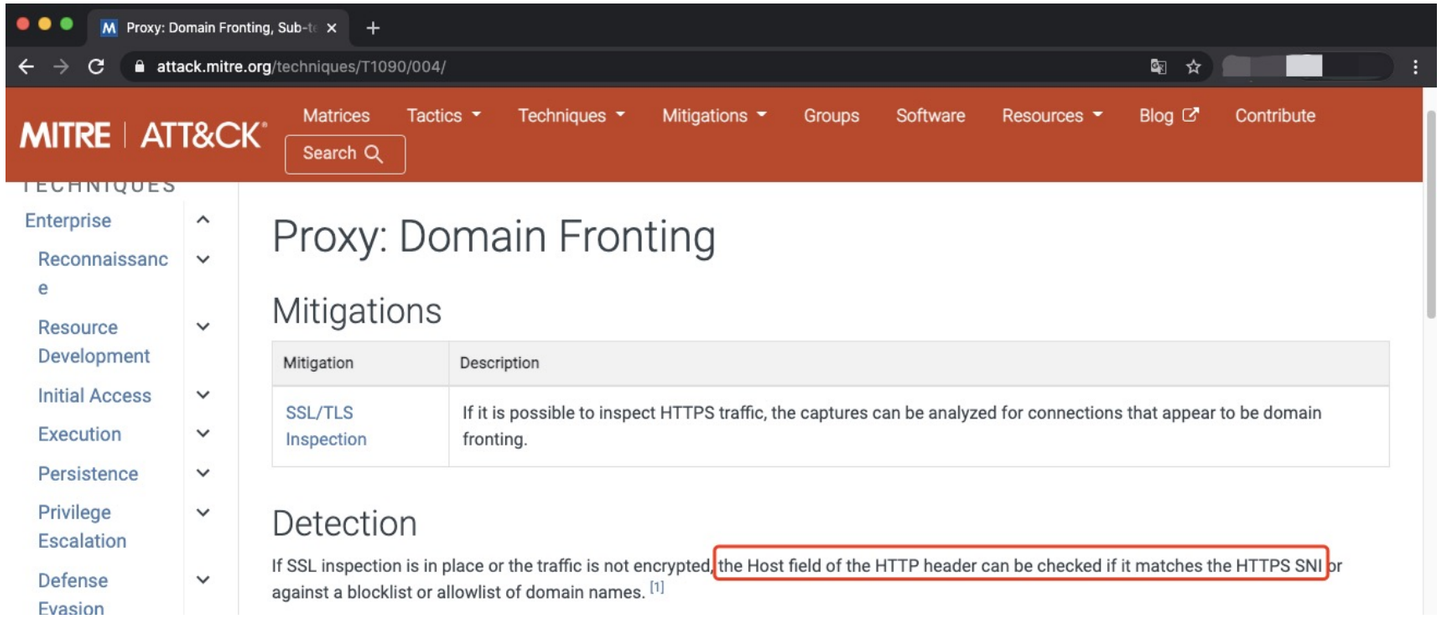
Domain Fronting

- Fifield, David; Lan, Chang; Hynes, Rod; Wegmann, Percy; Paxson, Vern. Blocking-resistant communication through domain fronting; 2015



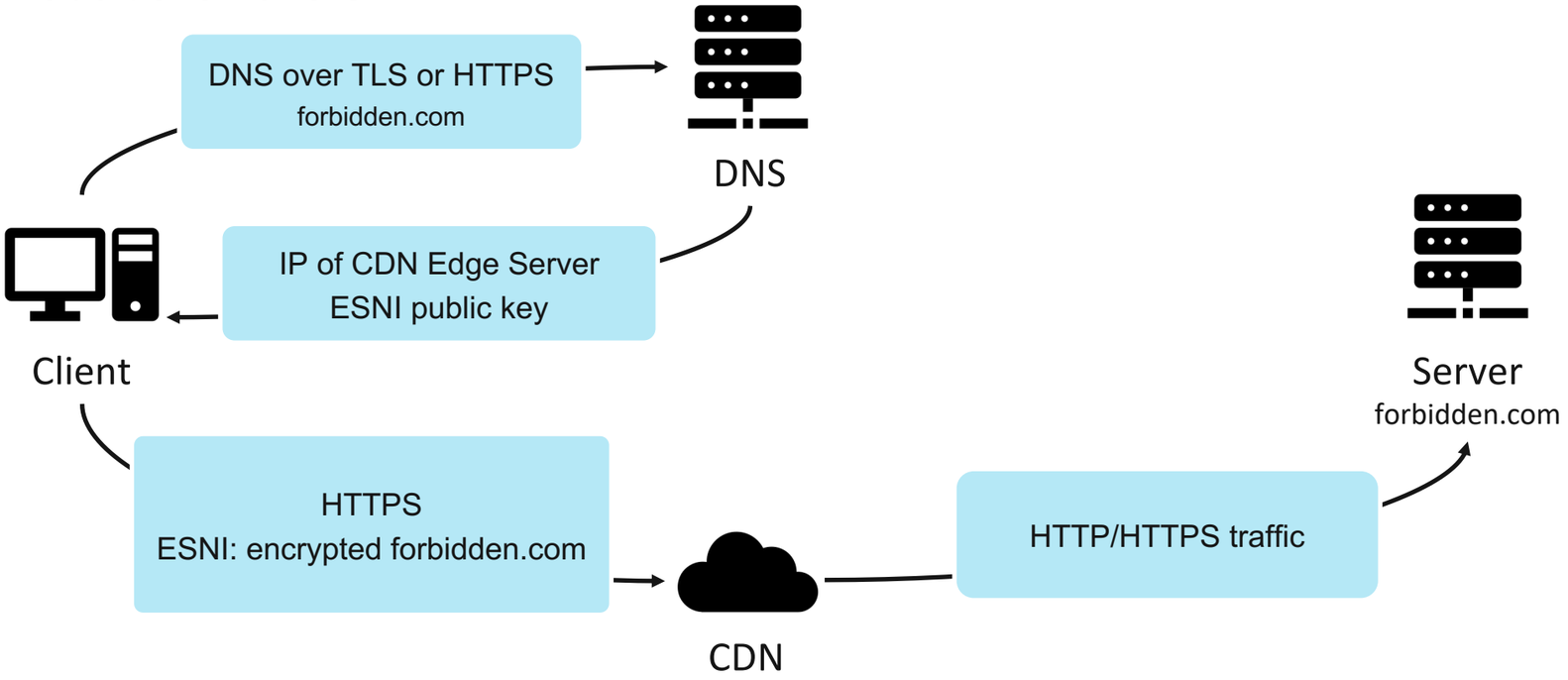
Domain Fronting - Limitations

- SNI != Host
  - Decrypt HTTPS traffic and check if SNI == Host
- Some CDN venders no longer support Domain Fronting



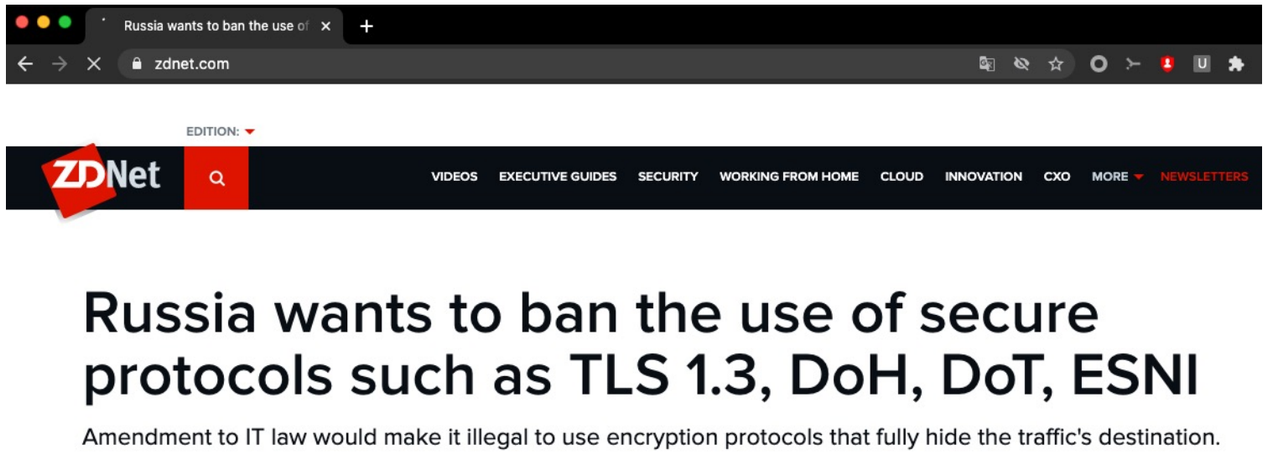
Domain Hiding

- Defcon 28 Erik Hunstad, Domain Fronting Is Dead, Long Live Domain Fronting, 2020
- Cloudflare TLS1.3 ESNI (IETF draft)
  - ESNI + an additional fake SNI



Domain Hiding - Limitations

- Cloudflare
  - Refused any Client Hello which has both ESNI and SNI
- TLS1.3 ESNI
  - Blocked in some enterprise environment
  - Some country-wide firewalls have blocked[1] / want to block ESNI



[1] https://en.wikipedia.org/wiki/Server_Name_Indication#Encrypted_Client_Hello

What we want for an ideal C2

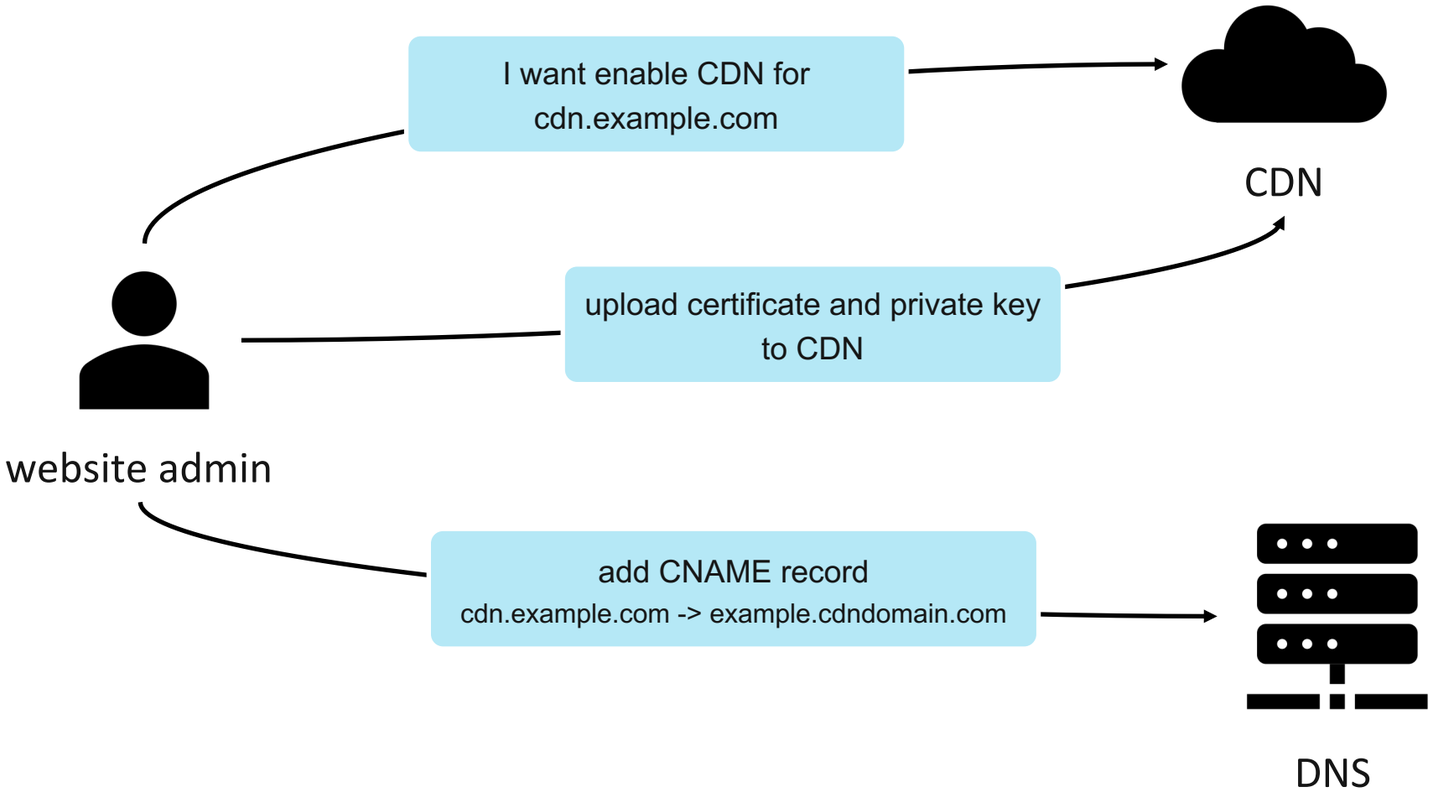
- A large number of IP addresses for C2
- Encrypted traffic (e.g. HTTPS)
- High-reputation domains with valid HTTPS certificates
- Even decrypted, the network traffic looks like normal HTTPS traffic (SNI == Host)
- Not be blocked in some specific districts

Outline

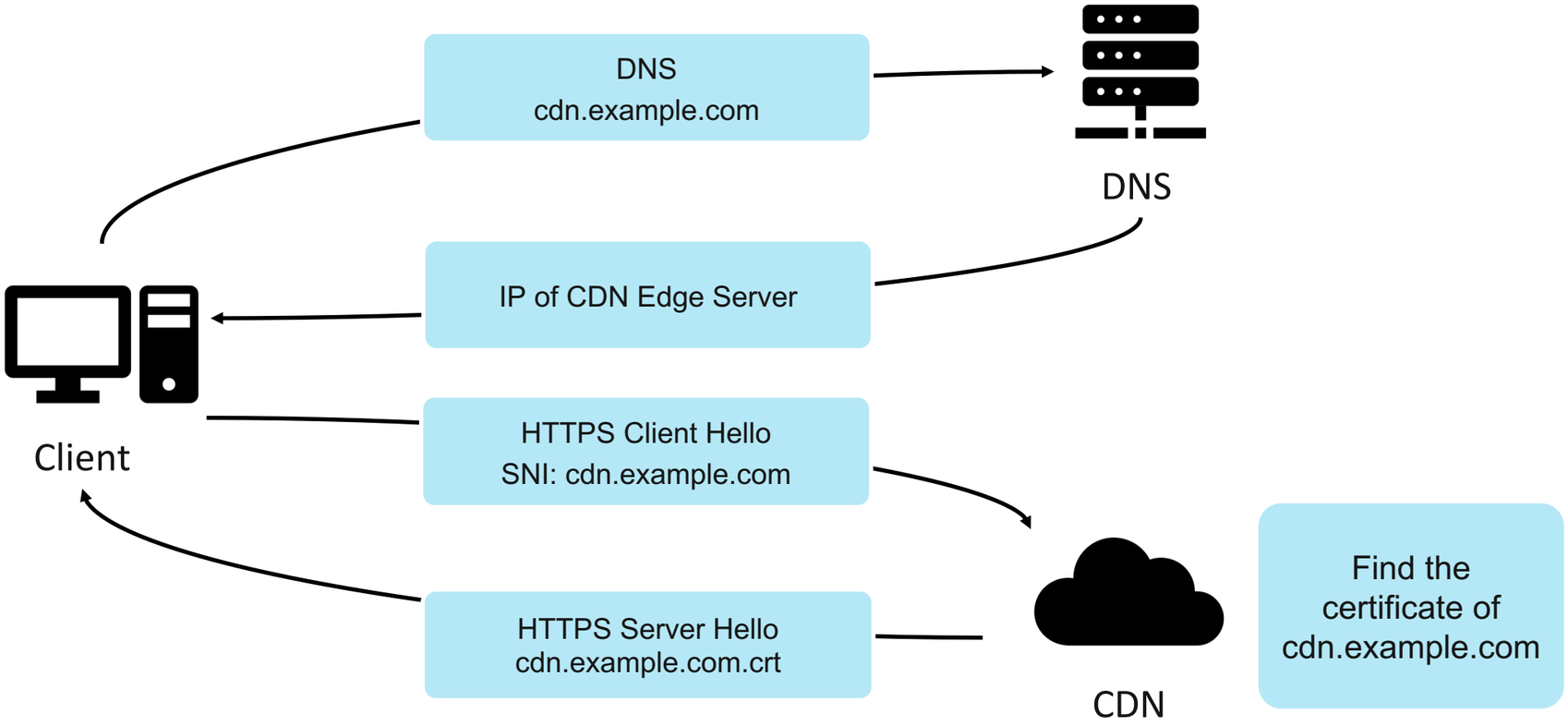
- Background & Previous Work
  - Domain Fronting
  - Domain Hiding with TLS1.3 and ESNI
- Domain Borrowing
  - The HTTPS CDN workflow
  - Borrow arbitrary domain
  - Borrow valid HTTPS certificates
- Detection & Mitigation
- Demo: Bypass Palo Alto Firewall

The HTTPS CDN workflow

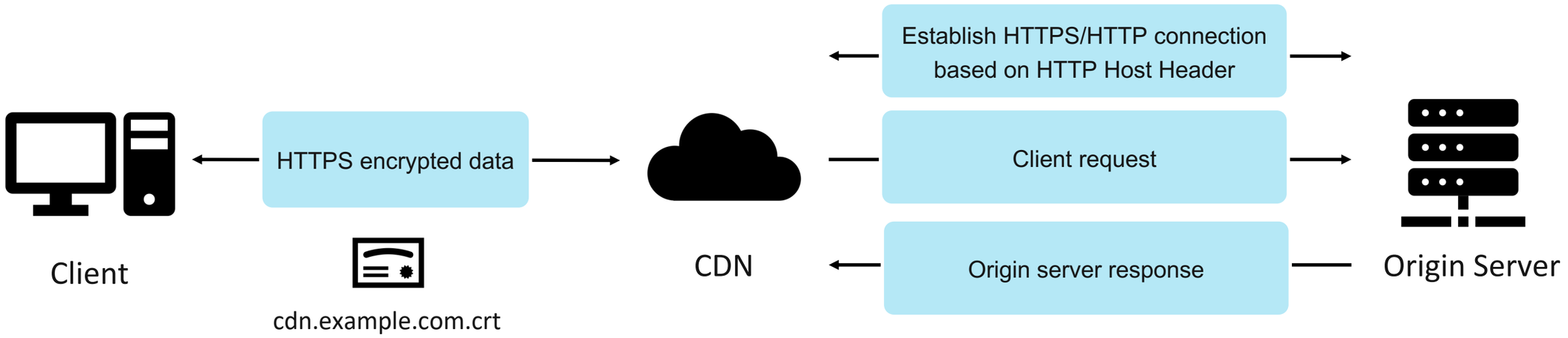
- CDN works like a man in the middle, it needs private keys of custom domains to decrypt HTTPS traffic



The HTTPS CDN workflow

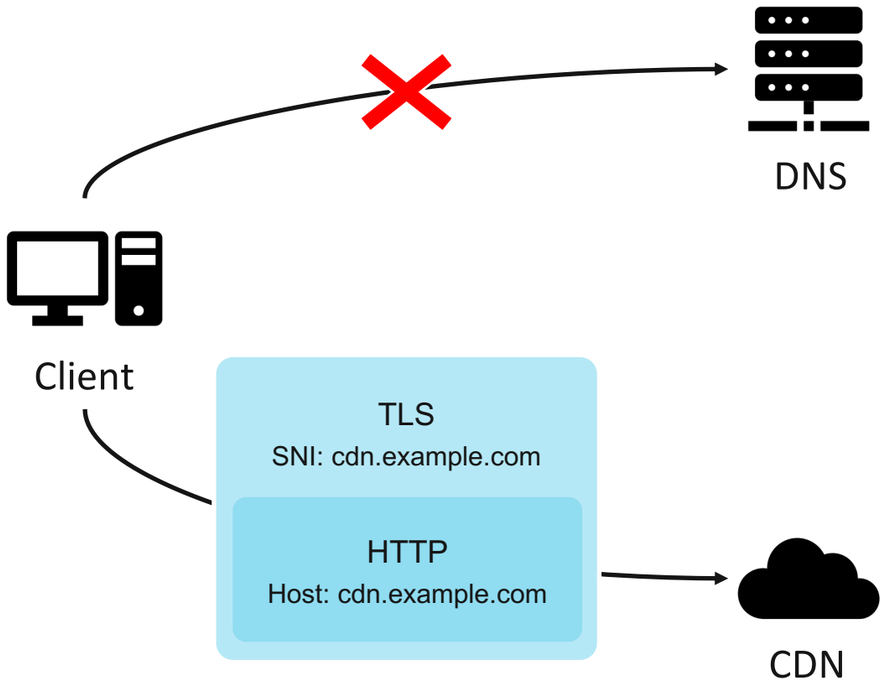


The HTTPS CDN workflow



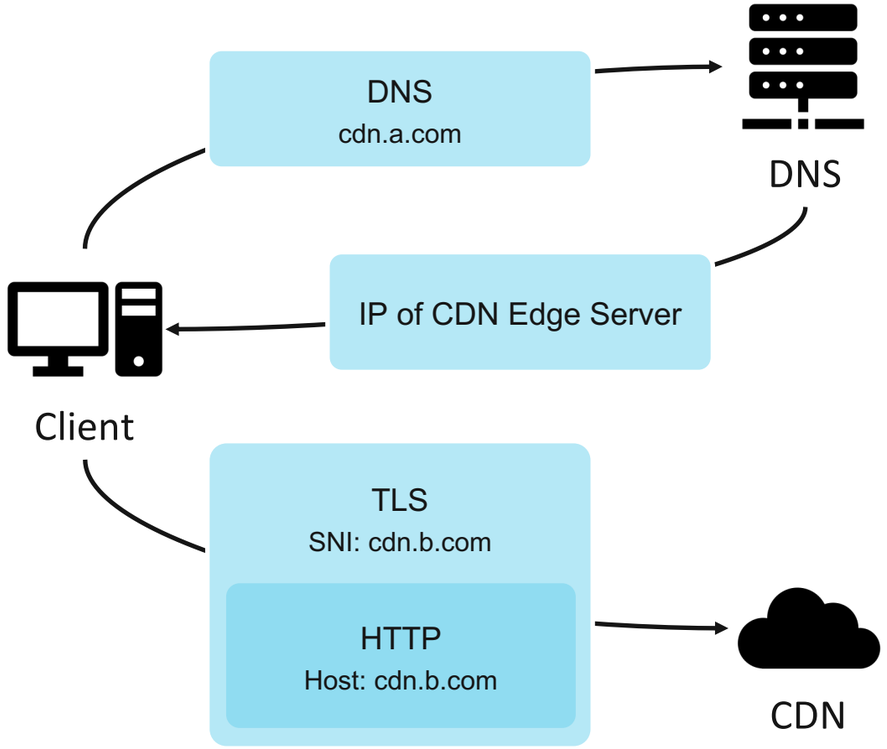
Domian Borrowing Basics – Abandon DNS

- DNS query is not a necessary condition for HTTPS connections
- Client can set an SNI in Client Hello and directly connect to IPs of CDN edge servers



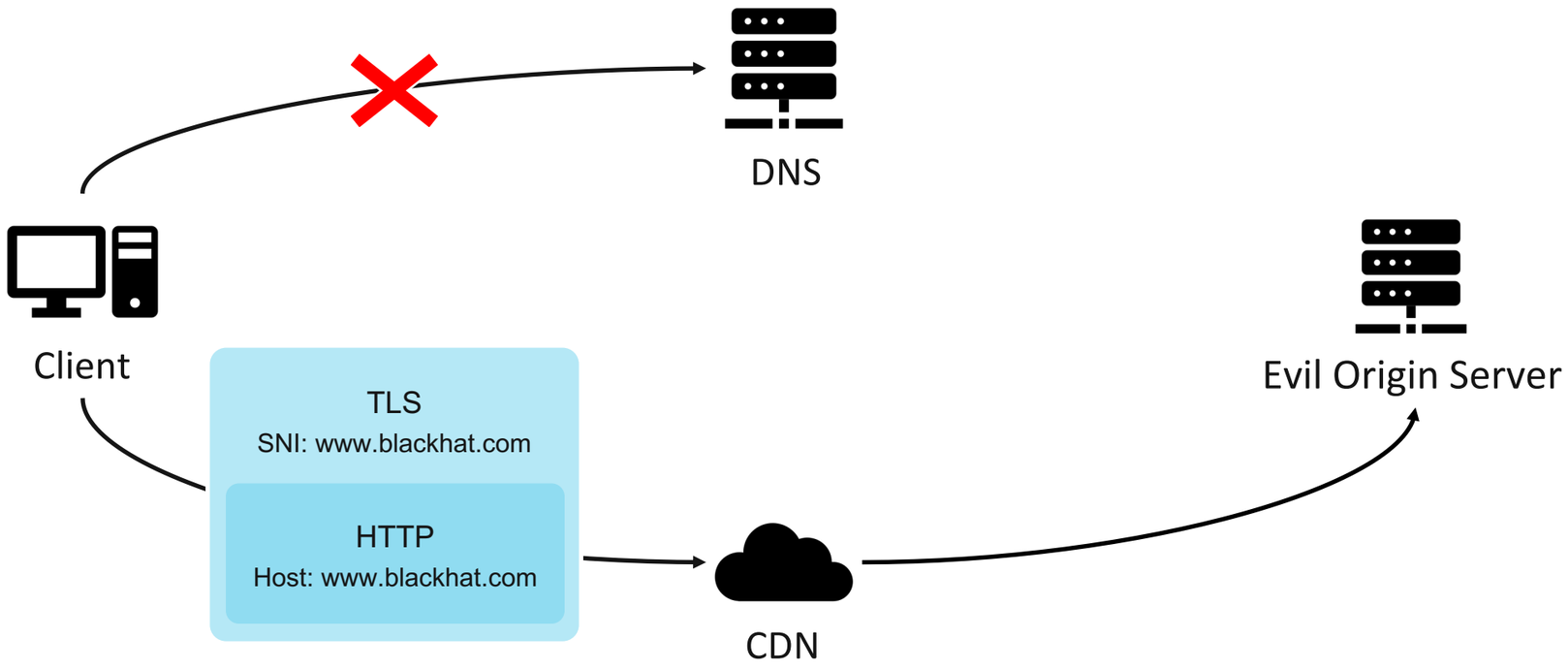
Domian Borrowing Basics – Abandon DNS

- Client can can use another CDN domain for DNS resolution



Domian Borrowing Basics – Domain Abusing

- Can we register an arbitrary domain in CDN?
- e.g. www.blackhat.com



CDN domain validation

	DNS	HTTPS certificate	AnyCast	None
AWS CloudFront		😀		
Azure CDN	😀			
Google Cloud CDN			😀	
Cloudflare	😀			
Fastly				😈
StackPath				😈
KeyCDN				😈
CDN77				😈
CDNSun				😈

Abusing CDN domain validation

- Register arbitrary domain in CDN

DOMAIN ▲

- accounts.google.com
- api.github.com
- api.twitter.com
- docs.microsoft.com
- onedrive.live.com
- www.blackhat.com
- www.office.com

Domains

Domains are used to route requests to your service. Customers associate their domain names with their origin (content source) when provisioning a Fastly service.

+ CREATE DOMAIN

cloud.amazonaws.com	Activate to test this domain.	
fonts.googleapis.com	Activate to test this domain.	
login.microsoftonline.com	Activate to test this domain.	
www.blackhat.com	Activate to test this domain.	
zoom.us	Activate to test this domain.	

When CDN can't find the certificate

- Most CDNs will send the default certificate to the client
- Some CDNs will send TCP RST to the client

```
curl https://www.blackhat.com --resolve www.blackhat.com:443:151.101.108.249 -k -v

……
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
*  subject: C=US; ST=California; L=San Francisco; O=Fastly, Inc.; CN=default.ssl.fastly.net
*  start date: Nov 12 16:01:03 2019 GMT
*  expire date: Jan  8 17:01:02 2022 GMT
*  subjectAltName does not match www.blackhat.com
* SSL: no alternative certificate subject name matches target host name 'www.blackhat.com'
……
```

Borrow arbitrary domain

- Register www.blackhat.com in CDN
- The client use www.blackhat.com to establish an HTTPS connection with CDN

- SNI == Host
  - Can bypass Domain Fronting detection
- Better than self-signed certificates, but still incorrect HTTPS certificates (default.ssl.fastly.net) 😿

Obtain valid HTTPS certificates

- Gain the power by hacking

Read the certificate and private key directly

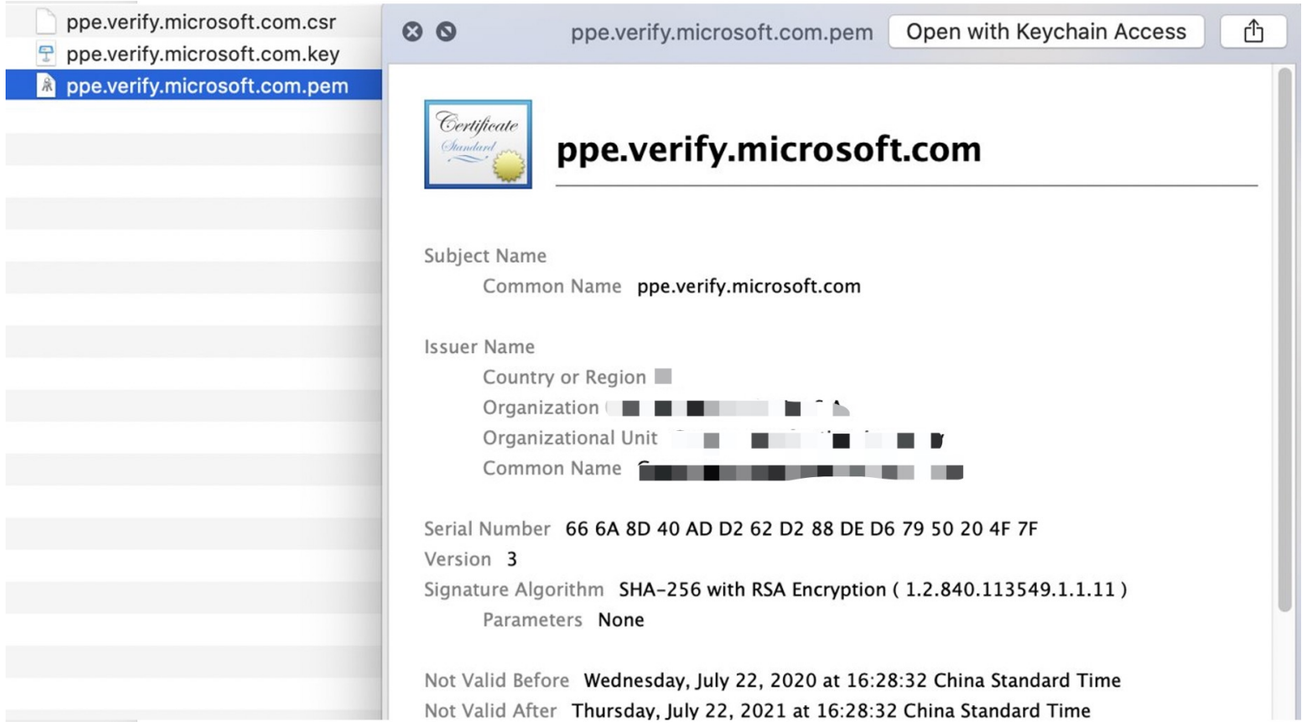
- Web application RCE
- Arbitrary file download
- ……

Apply for a new HTTPS certificate with HTTP-based validation (.well-known)

- Web application RCE
- Subdomain takeover
- Arbitrary file upload, especially upload to cloud storage
- ……

Obtain valid HTTPS certificates

- Subdomain takeover: ppe.verify.microsoft.com [1]
- Apply for a HTTPS certificate/private key of ppe.verify.microsoft.com




```
ubuntu@xuanwu-lab:~$ curl http://ppe.verify.microsoft.com/ -I
HTTP/1.1 301 Moved Permanently
Date: Thu, 25 Mar 2021 10:29:02 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
Location: https://redirect.microsoft/
```

[1] ppe.verify.microsoft.com subdomain takeover was found by a friend of ours

CDN domain validation bypass

- AWS CloudFront validates the CDN domain only by the HTTPS certificate.

Alternate Domain Names (CNAMEs) ppe.verify.microsoft.com

SSL Certificate

○ Default CloudFront Certificate (*.cloudfront.net)

Choose this option if you want your users to use HTTPS or HTTP to access your content with the CloudFront domain name (such as https://d111111abcdef8.cloudfront.net/logo.jpg).
Important: If you choose this option, CloudFront requires that browsers or devices support TLSv1 or later to access your content.

◉ Custom SSL Certificate (example.com):

Choose this option if you want your users to access your content by using an alternate domain name, such as https://www.example.com/logo.jpg.
You can use a certificate stored in AWS Certificate Manager (ACM) in the US East (N. Virginia) Region, or you can use a certificate stored in IAM.

ppe.verify.microsoft.com (5ee469e3-b55

Request or Import a Certificate with ACM

Learn more about using custom SSL/TLS certificates with CloudFront.
Learn more about using ACM.

CDN domain validation bypass

- We can register ppe.verify.microsoft.com in AWS CloudFront

Viewing certificates 1 to 2

Name	Domain name	Additional names	Status	Type	In use?	Renewal eligibility
-	ppe.verify.microsoft.com	-	Issued	Imported	Yes	Ineligible

Status

Status Issued
Detailed status The cert was imported at 2020-12-11T05:30:35UTC

Reimport certificate

Details

Type Imported
In use? Yes
Domain name ppe.verify.microsoft.com
Imported at 2020-12-11T05:30:35UTC
Not after 2021-07-22T08:28:32UTC
Expires in 216 Days

CloudFront Distributions

Create Distribution | Distribution Settings | Delete | Enable | Disable

Viewing : Any Delivery Method | Any State

Viewing 1 to 1 of 1 Items

Delivery Method	ID	Domain Name	Comme	Origin	CNAMEs	Status	State	Last Modified
Web	E1XY6KK4	d2o8515f9163be.clou	-		ppe.verify.microsoft.com	Deployed	Enabled	2020-12-17 17:49 UT

C2 agent with “Microsoft” traffic

- Demo
  - Covenant C2 with a customed ImplantTemplate
  - DNS: blogs.aws.amazon.com
  - SNI == Host == ppe.verify.microsoft.com
  - Apply for a valid certificate through subdomain takeover
  - Register CDN domain (ppe.verify.microsoft.com) in AWS CloudFront

Capturing from vmnet8

tls.handshake.type == 1 || tls.handshake.type == 2

No.	Time	Source	Destination	Protocol	Length	Info
55	49.989929	192.168.2.131	13.225.93.71	TLSv1.2	234	Client Hello
59	50.044078	13.225.93.71	192.168.2.131	TLSv1.2	1342	Server Hello
79	50.534396	192.168.2.131	13.225.93.71	TLSv1.2	370	Client Hello
81	50.592371	13.225.93.71	192.168.2.131	TLSv1.2	197	Server Hello, Change Cipher Spec, Encrypted Handshake Message
97	51.466191	192.168.2.131	13.225.93.71	TLSv1.2	370	Client Hello
99	51.520787	13.225.93.71	192.168.2.131	TLSv1.2	197	Server Hello, Change Cipher Spec, Encrypted Handshake Message
111	51.837201	192.168.2.131	13.225.93.71	TLSv1.2	370	Client Hello
113	51.892624	13.225.93.71	192.168.2.131	TLSv1.2	197	Server Hello, Change Cipher Spec, Encrypted Handshake Message
198	52.981239	192.168.2.131	13.225.93.56	TLSv1.2	370	Client Hello
200	53.026434	13.225.93.56	192.168.2.131	TLSv1.2	197	Server Hello, Change Cipher Spec, Encrypted Handshake Message
212	53.348880	192.168.2.131	13.225.93.56	TLSv1.2	370	Client Hello
214	53.395853	13.225.93.56	192.168.2.131	TLSv1.2	197	Server Hello, Change Cipher Spec, Encrypted Handshake Message

```
    Cipher Suites Length: 42
  ▶ Cipher Suites (21 suites)
    Compression Methods Length: 1
  ▶ Compression Methods (1 method)
    Extensions Length: 88
  ▼ Extension: server_name (len=29)
      Type: server_name (0)
      Length: 29
    ▼ Server Name Indication extension
        Server Name list length: 27
        Server Name Type: host_name (0)
        Server Name length: 24
        Server Name: ppe.verify.microsoft.com
  ▼ Extension: supported_groups (len=8)
      Type: supported_groups (10)
      Length: 8
      Supported Groups List Length: 6
    ▶ Supported Groups (3 groups)
  ▼ Extension: ec_point_formats (len=2)
      Type: ec_point_formats (11)
      Length: 2
```

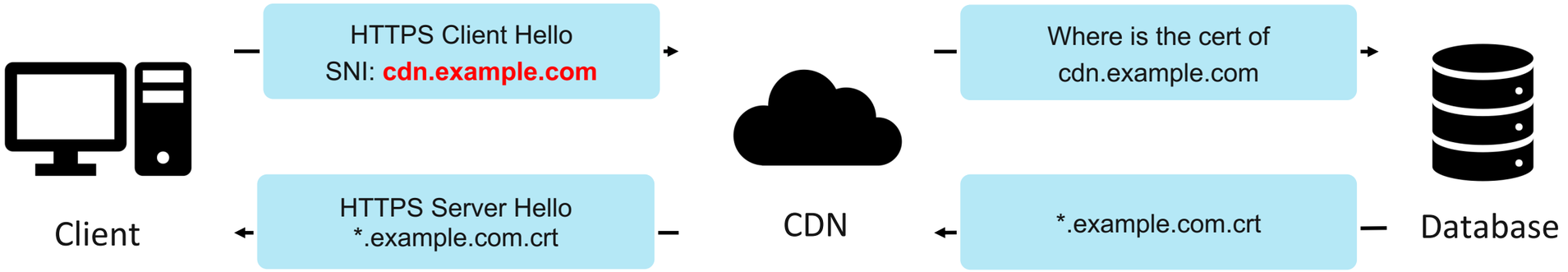
```
0000  00 50 56 e4 7b e8 00 0c  29 e5 ba 7a 08 00 45 00   ·PV·{··· )··z··E·
0010  00 dc 7d d9 40 00 80 06  4d ef c0 a8 02 83 0d e1   ··}·@··· M·******
0020  5d 47 cc e1 01 bb 77 a8  32 9c b9 42 77 5b 50 18   ]G····w· 2··Bw[P·
0030  fa f0 ca 95 00 00 16 03  03 00 af 01 00 00 ab 03   ********  ********
0040  03 60 65 34 a2 23 9a a4  bc 6d 00 ca 26 0c d1 73   ·`e4·#·· ·m··&··s
0050  61 e3 65 8f 81 00 17 08  45 8d 3b 1a c6 c1 f8 4a   a·e····· E·;····J
0060  b8 00 00 2a c0 2c c0 2b  c0 30 c0 2f 00 9f 00 9e   ···*·,·+ ·0·/····
0070  c0 24 c0 23 c0 28 c0 27  c0 0a c0 09 c0 14 c0 13   ·$·#·(·' ********
0080  00 9d 00 9c 00 3d 00 3c  00 35 00 2f 00 0a 01 00   *****=·< ·5·/····
0090  00 58 00 00 00 1d 00 1b  00 00 18 70 70 65 2e 76   ·X****** ***ppe.v
00a0  65 72 69 66 79 2e 6d 69  63 72 6f 73 6f 66 74 2e   erify.mi crosoft.
00b0  63 6f 6d 00 0a 00 08 00  06 00 1d 00 17 00 18 00   com***** ********
00c0  0b 00 02 01 00 00 0d 00  14 00 12 04 01 05 01 02   ******** ********
00d0  01 04 03 05 03 02 03 02  02 06 01 06 03 00 23 00   ******** ******#·
00e0  00 00 17 00 00 ff 01 00  01 00                     ******** ··
```

0:50.11

How to obtain valid HTTPS certificates without hacking🤔

CDN HTTPS certificates distribution

- Correct way to distribute wildcard HTTPS certificates

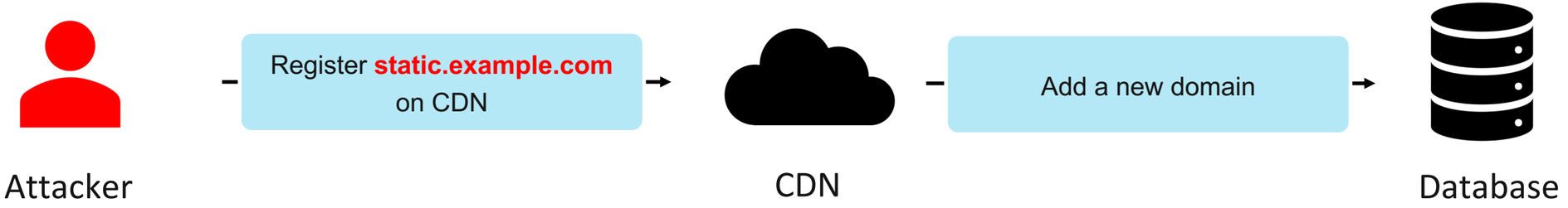


select certificate from db where domain_name = **"cdn.example.com"**

cdn user	domain name	certificate
alice	**cdn.example.com**	***.example.com.crt**
bob	cdn.a.com	cdn.a.com.crt
	……	……

CDN HTTPS certificates distribution

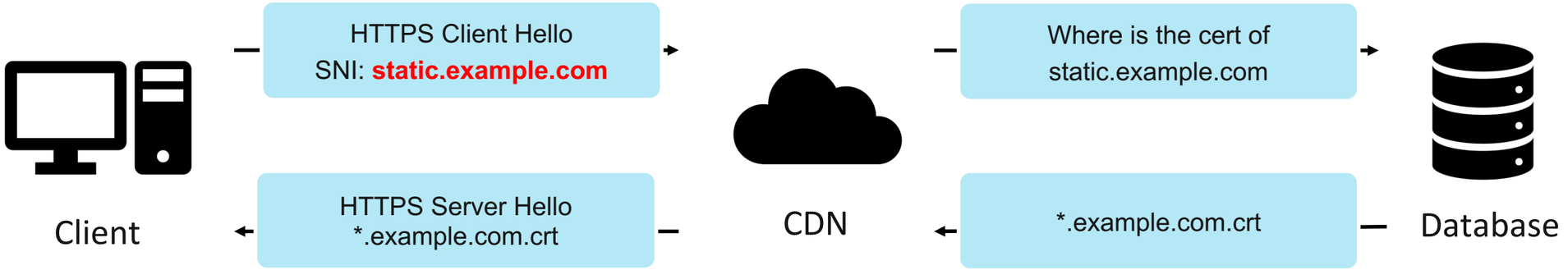
- Some CDNs improperly implement wildcard HTTPS certificates distribution



cdn user	domain name	certificate
alice	cdn.example.com	*.example.com.crt
bob	cdn.a.com	cdn.a.com.crt
attacker	**static.example.com**	**NULL**
……	……	……

CDN HTTPS certificates distribution

- Attackers can borrow subdomains and wildcard HTTPS certificates from other users



select certificate from db where **certificate matches "static.example.com"**

cdn user	domain name	certificate
alice	cdn.example.com	***.example.com.crt**
bob	cdn.a.com	cdn.a.com.crt
attacker	**static.example.com**	NULL
……	……	……

attacker borrows alice's certificate

Borrow valid HTTPS certificates

- We can borrow wildcard HTTPS certificates on StackPath and CDN77

STACKPATH™

CDN77.com
Content Delivery Network

Borrow valid HTTPS certificates

- Lots of well-known domains with wildcard HTTPS certificates are on StackPath / CDN77
  - *.bootstrapcdn.com
  - *.fontawesome.com
  - *.xvideos-cdn.com 🙈
  - …….

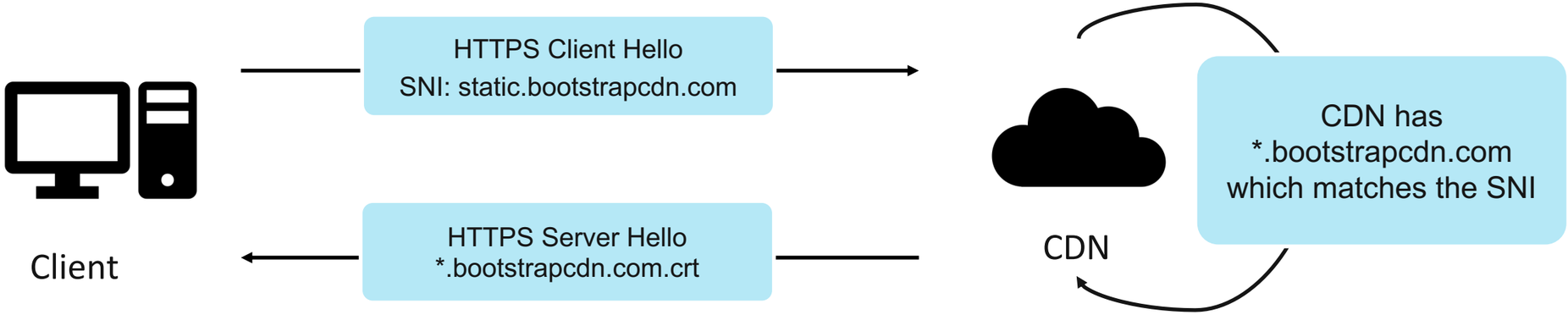
JS Foundation

Font Awesome

B Bootstrap

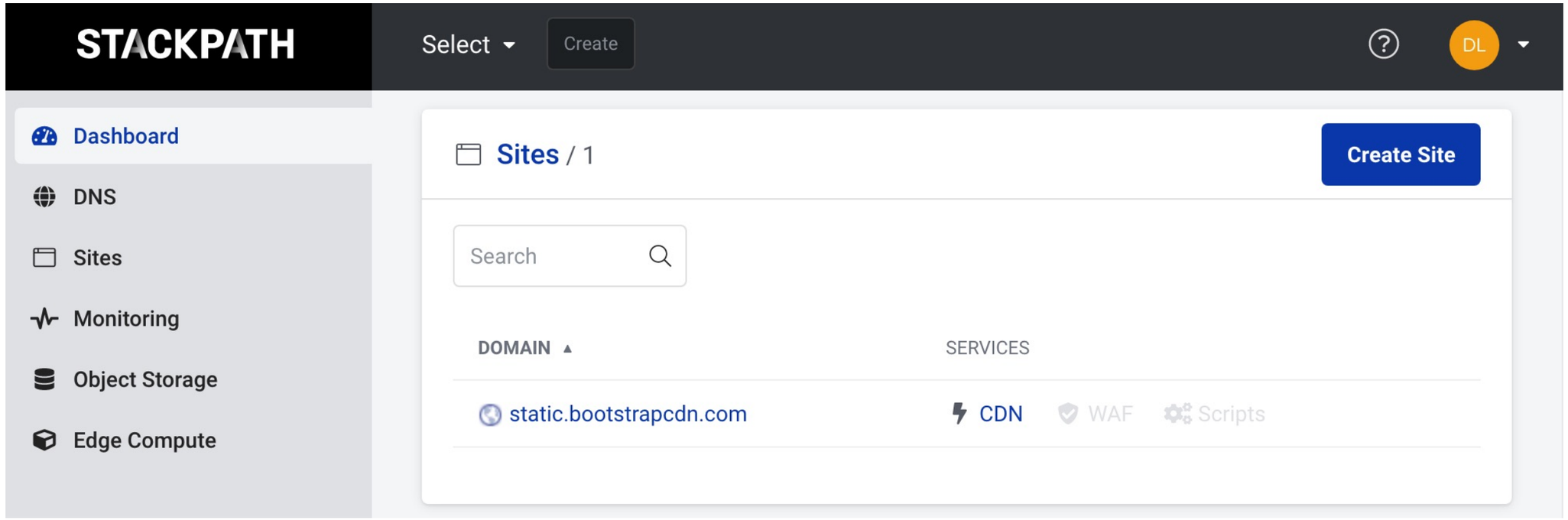
Borrow valid HTTPS certificates

- We can register any subdomain of bootstrapcdn.com
  - even a non-existent domain
- e.g. static.bootstrapcdn.com



Borrow valid HTTPS certificates

- static.bootstrapcdn.com on StackPath



Borrow valid HTTPS certificates

- static.bootstrapcdn.com

```
ubuntu@xuanwu-lab:~$ dig static.bootstrapcdn.com

; <<>> DiG 9.16.1-Ubuntu <<>> static.bootstrapcdn.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 39473
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;static.bootstrapcdn.com.       IN      A

;; Query time: 8 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Wed Mar 31 11:55:48 CST 2021
;; MSG SIZE  rcvd: 52
```

```
ubuntu@xuanwu-lab:~$ curl https://static.bootstrapcdn.com/test.php --resolve static.bootstrapcdn.com:
443:151.139.128.11 -v
* Added static.bootstrapcdn.com:443:151.139.128.11 to DNS cache
* Hostname static.bootstrapcdn.com was found in DNS cache
*   Trying 151.139.128.11:443...
* TCP_NODELAY set
* Connected to static.bootstrapcdn.com (151.139.128.11) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: /etc/ssl/certs
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_128_GCM_SHA256
* ALPN, server accepted to use h2
* Server certificate:
*  subject: CN=*.bootstrapcdn.com
*  start date: Sep 22 00:00:00 2020 GMT
*  expire date: Oct 12 23:59:59 2021 GMT
*  subjectAltName: host "static.bootstrapcdn.com" matched cert's "*.bootstrapcdn.com"
*  issuer: C=GB; ST=Greater Manchester; L=Salford; O=Sectigo Limited; CN=Sectigo RSA Domain Validatio
n Secure Server CA
*  SSL certificate verify ok.
```

C2 agent with “Bootstrap” traffic

- Demo
  - Covenant C2 with a customed ImplantTemplate
  - DNS: www.stackpath.com
  - SNI == Host == static.bootstrapcdn.com
  - Register CDN domain (static.bootstrapcdn.com) in StackPath
  - Valid HTTPS certificate (*.bootstrapcdn.com)

Capturing from vmnet8

tls.handshake.type == 1 || tls.handshake.type == 2

No.	Time	Source	Destination	Protocol	Length	Info
30	112.205398	192.168.2.131	151.139.128.11	TLSv1.2	233	Client Hello
32	112.333436	151.139.128.11	192.168.2.131	TLSv1.2	1342	Server Hello
51	112.578234	192.168.2.131	151.139.128.11	TLSv1.2	393	Client Hello
53	112.629091	151.139.128.11	192.168.2.131	TLSv1.2	159	Server Hello, Change Cipher Spec, Encrypted Handshake Message
65	113.062278	192.168.2.131	151.139.128.11	TLSv1.2	393	Client Hello
67	113.113158	151.139.128.11	192.168.2.131	TLSv1.2	159	Server Hello, Change Cipher Spec, Encrypted Handshake Message
81	113.528636	192.168.2.131	151.139.128.11	TLSv1.2	393	Client Hello
83	113.577816	151.139.128.11	192.168.2.131	TLSv1.2	159	Server Hello, Change Cipher Spec, Encrypted Handshake Message
164	114.628960	192.168.2.131	151.139.128.11	TLSv1.2	393	Client Hello
166	114.677747	151.139.128.11	192.168.2.131	TLSv1.2	159	Server Hello, Change Cipher Spec, Encrypted Handshake Message
178	115.086714	192.168.2.131	151.139.128.11	TLSv1.2	393	Client Hello
180	115.129351	151.139.128.11	192.168.2.131	TLSv1.2	159	Server Hello, Change Cipher Spec, Encrypted Handshake Message

```
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 61
    ▼ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 57
        Version: TLS 1.2 (0x0303)
      ▶ Random: 848dd70c19b14d53f59c193ec03d2addc9eb535508f4edec444f574e47524401
        Session ID Length: 0
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Compression Method: null (0)
        Extensions Length: 17
      ▼ Extension: renegotiation_info (len=1)
          Type: renegotiation_info (65281)
          Length: 1
        ▼ Renegotiation Info extension
            Renegotiation info extension length: 0
      ▼ Extension: ec_point_formats (len=4)
          Type: ec_point_formats (11)
```

```
0030  fa f0 e7 43 00 00 16 03  03 00 3d 02 00 00 39 03   ···C···· ··=···9·
0040  03 84 8d d7 0c 19 b1 4d  53 f5 9c 19 3e c0 3d 2a   ·******M S···>·=*
0050  dd c9 eb 53 55 08 f4 ed  ec 44 4f 57 4e 47 52 44   ···SU··· ·DOWNGRD
0060  01 00 c0 2f 00 00 11 ff  01 00 01 00 00 0b 00 04   ···/···· ********
0070  03 00 01 02 00 23 00 00  16 03 03 15 ae 0b 00 15   *****#·· ********
0080  aa 00 15 a7 00 05 c9 30  82 05 c5 30 82 04 ad a0   *******0 ···0····
0090  03 02 01 02 02 10 39 6c  45 e1 93 57 f3 c7 e2 38   ******9l E··W···8
00a0  f4 1c 80 0e 97 7f 30 0d  06 09 2a 86 48 86 f7 0d   ******0· ··*·H···
00b0  01 01 0b 05 00 30 81 8f  31 0b 30 09 06 03 55 04   *****0·· 1·0···U·
00c0  06 13 02 47 42 31 1b 30  19 06 03 55 04 08 13 12   ···GB1·0 ···U····
00d0  47 72 65 61 74 65 72 20  4d 61 6e 63 68 65 73 74   Greater  Manchest
00e0  65 72 31 10 30 0e 06 03  55 04 07 13 07 53 61 6c   er1·0··· U····Sal
00f0  66 6f 72 64 31 18 30 16  06 03 55 04 0a 13 0f 53   ford1·0· ··U····S
0100  65 63 74 69 67 6f 20 4c  69 6d 69 74 65 64 31 37   ectigo L imited17
0110  30 35 06 03 55 04 03 13  2e 53 65 63 74 69 67 6f   05··U··· .Sectigo
0120  20 52 53 41 20 44 6f 6d  61 69 6e 20 56 61 6c 69    RSA Dom ain Vali
0130  64 61 74 69 6f 6e 20 53  65 63 75 72 65 20 53 65   dation S ecure Se
0140  72 76 65 72 20 43 41 30  1e 17 0d 32 30 30 39 32   rver CA0 ···20092
0150  32 30 30 30 30 30 30 5a  17 0d 32 31 31 30 31 32   2000000Z ··211012
0160  32 33 35 39 35 39 5a 30  1d 31 1b 30 19 06 03 55   235959Z0 ·1·0···U
0170  04 03 0c 12 2a 2e 62 6f  6f 74 73 74 72 61 70 63   ····*.bo otstrapc
0180  64 6e 2e 63 6f 6d 30 82  01 22 30 0d 06 09 2a 86   dn.com0· ·"0···*·
0190  48 86 f7 0d 01 01 01 05  00 03 82 01 0f 00 30 82   H******· ******0·
01a0  01 0a 02 82 01 01 00 e7  5d c0 8a 20 bb d9 ae d7   ******** ]·· ····
01b0  84 6b 12 b2 c0 83 fa 70  53 23 c6 c2 c6 2b ad 2e   ·k·····p S#···+··
01c0  66 a4 17 1c bb 4a 5c 3d  d4 dd be dc c9 ec 2a 25   f····J\= *******%
01d0  94 d3 be c9 34 11 a3 5f  23 d0 be 6d ca 3f cd 50   ····4··_ #··m·?·P
```

0:58.00

Domain Borrowing

- Register high-reputation domains on CDN
- Borrow valid HTTPS certificates
  - certificates from vulnerable websites
  - wildcard certificates from other CDN users
- Then combine them to hide your C2 traffic to circumvent censorship

Domain Borrowing vs. Others

Detection method	Domain Borrowing	Domain Fronting	Domain Hiding
high reputation SNI	✅	✅	✅
high reputation Host	✅	❌	--- [2]
check if SNI == Host	✅	❌	--- [2]
valid HTTPS certificates	✅	✅	✅
without ESNI[1]	✅	✅	❌

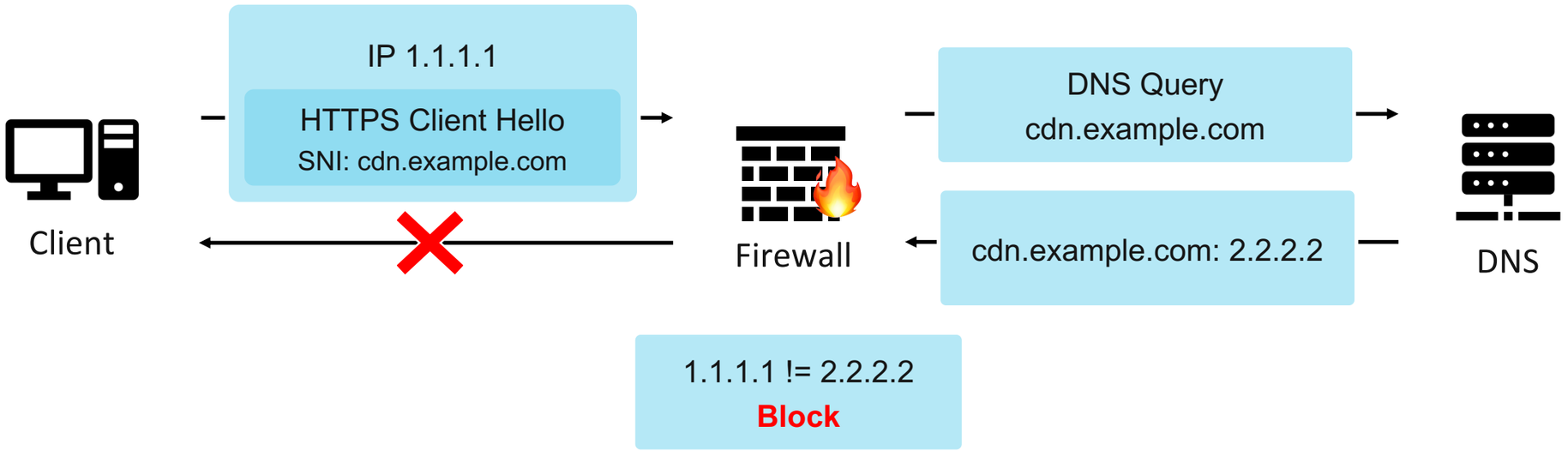
[1] ESNI will be blocked by some country-wide and enterprise firewalls
[2] TLSv1.3 + ESNI cannot be decrypted by well-known firewalls currently

Outline

- Background & Previous Work
  - Domain Fronting
  - Domain Hiding with TLS1.3 and ESNI
- Domain Borrowing
  - The HTTPS CDN workflow
  - Borrow arbitrary domain
  - Borrow valid HTTPS certificates
- Detection & Mitigation
- Demo: Bypass Palo Alto Firewall

Detection

- Check if DNSLookup(SNI) == IP.dst



Mitigation

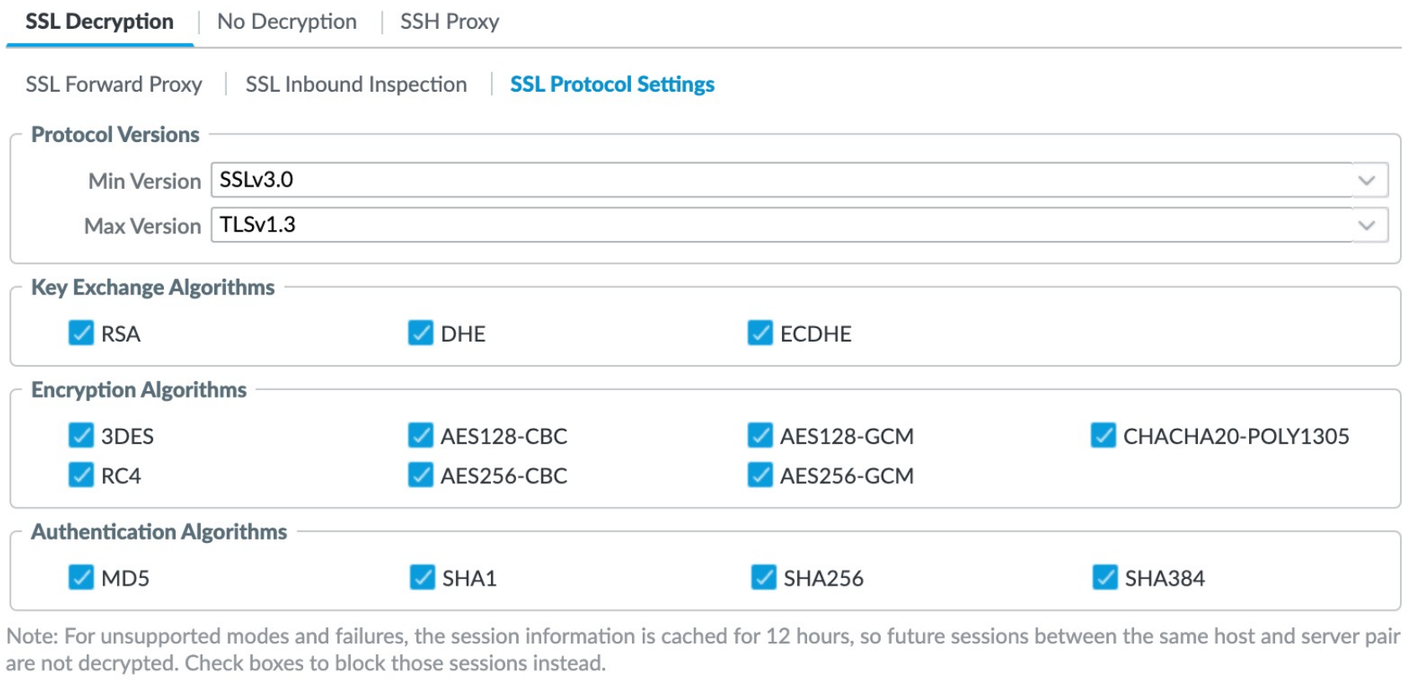
- For CDN vendors
  - Validate the custom domain strictly
    - DNS records is a better than HTTPS certificates
  - Distribute wildcard HTTPS certificates correctly
- For website admins
  - Certificate Revocation, If attackers steal your HTTPS certificates
  - Certificate Transparency, If attackers applied for new HTTPS certificates of your domains

Outline

- Background & Previous Work
  - Domain Fronting
  - Domain Hiding with TLS1.3 and ESNI
- Domain Borrowing
  - The HTTPS CDN workflow
  - Borrow arbitrary domain
  - Borrow valid HTTPS certificates
- Detection & Mitigation
- Demo: Bypass Palo Alto Firewall

Palo Alto Firewall

- PAN-VM 10.0.4
  - Next-Generation and HTTPS Decryption Firewall
  - Supports SSLv3.0 – TLSv1.3 decryption



Palo Alto Firewall

- Anti-Spyware Evasion Signatures [1]
  - Suspicious HTTP Evasion Found
    - DNSLookup(HOST) != IP.dst
  - Suspicious TLS Evasion Found
    - DNSLookup(SNI) != IP.dst

Signature Policies | **Signature Exceptions** | DNS Policies | DNS Exceptions

evasion 2 / 13912

ENA...	ID	THREAT NAME	IP ADDRESS EXEMPTIONS	POLICY	CATEGORY	SEVERITY	ACTION	PACKET CAPTURE
☐	14978	Suspicious TLS Evasion Found		alert-all	spyware	informational	default (allow)	disable
☐	14984	Suspicious HTTP Evasion Found		alert-all	spyware	informational	default (allow)	disable

[1] https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/threat-prevention/enable-evasion-signatures.html

Palo Alto Firewall

- Anti-Spyware Evasion Signatures
  - Can detect domain borrowing theoretically
  - But with improper implementation 😈

Bypass Palo Alto Firewall

- Anti-Spyware Evasion Signatures feature
  - passthrough if Palo Alto Firewall cannot resolve the domain in SNI/Host

- Domain Borrowing
  - The SNI can be any domain, even a non-existent domain
  - Bypass Anti-Spyware Evasion Signatures

Bypass Palo Alto Firewall

- Demo
  - Covenant C2 with customed ImplantTemplate
  - DNS: staging.fontawesome.com
  - SNI == Host == img.fontawesome.com
  - Register CDN domain (img.fontawesome.com) in StackPath
  - Valid HTTPS certificate (*.fontawesome.com)

```
ubuntu@xuanwu-lab:~$ dig img.fontawesome.com

; <<>> DiG 9.16.1-Ubuntu <<>> img.fontawesome.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 26310
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;img.fontawesome.com.           IN      A

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Mar 23 17:50:35 CST 2021
;; MSG SIZE  rcvd: 48
```

PA-VM | Covenant | Covenant

panos/?#monitor::vsys1::monitor/logs/decryption

PA-VM

DASHBOARD | ACC | MONITOR | POLICIES | OBJECTS | NETWORK | DEVICE

Commit

Manual

- Logs
  - Traffic
  - Threat
  - URL Filtering
  - WildFire Submissions
  - Data Filtering
  - HIP Match
  - GlobalProtect
  - IP-Tag
  - User-ID
  - Decryption
  - Tunnel Inspection
  - Configuration
  - System
  - Alarms
  - Authentication
  - Unified
- Packet Capture
- App Scope
  - Summary
  - Change Monitor
  - Threat Monitor
  - Threat Map
  - Network Monitor
  - Traffic Map
- Session Browser
- Botnet
- PDF Reports
  - Manage PDF Summary
  - User Activity Report
  - SaaS Application Usage
  - Report Groups
  - Email Scheduler
- Manage Custom Reports
- Reports

RECEIVE TIME	APPLICATI...	POLICY NAME	SERVER NAME INDICATION	SUBJECT COMMON NAME	ISSUER COMMON NAME	SOURCE ADDRESS	DESTINATI ADDRESS
03/31 00:24:54	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:24:53	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:24:52	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:24:51	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:24:49	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:24:48	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:24:47	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:24:45	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:24:41	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:24:40	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:24:39	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:24:39	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:24:39	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:24:35	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:24:35	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:24:34	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:21:59	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:21:57	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:21:56	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.
03/31 00:21:55	web-browsing	decrypt-all	img.fontawesome.com	*.fontawesome.com	DigiCert TLS RSA SHA256 2020 CA1	192.168.101.59	151.139.128.

Windows 10 x64 - VMware Workstation

C:\Users\xlab\Desktop\新建文件夹\img.fontawesome.com.exe

```
============================ HTTP REQ ============================
GET /api/message.php?id=a50df39648 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36
Host: img.fontawesome.com
Accept: */*
Accept-Language: en
Connection: close
==================== ============================
HTTP/1.1 200 OK
Date: Wed, 31 Mar 20
Accept-Ranges: bytes
Content-Type: text/p
X-HW: 1617175497.cds                                175497.cds024.hk1.p
Server: Nginx
Cache-Control: max-a
Access-Control-Allow
Connection: close
Content-Length: 0
```

计算器 — 标准 — 0

1:32.83

Domain Borrowing Implant Template: https://github.com/Dliv3/DomainBorrowing

Thank you

Q & A