



Offensive JA3

Max Harley

Shout Out

- Lee Christensen (@tifkin_)
- Matt Rinaldi (@mmaekr)
- John Althouse (@4A4133)
- Jeff Atkinson
- Josh Atkins
- Refraction.Networking

JA3

- <https://github.com/salesforce/ja3>



- ▼ Transport Layer Security
 - ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 161
 - ▼ Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 157
 - Version: TLS 1.2 (0x0303)
 - ▶ Random: 52362c1012cf23628256e745e903cea696e9f62a60ba0ae8...
 - Session ID Length: 0
 - Cipher Suites Length: 4
 - ▶ Cipher Suites (2 suites)
 - Compression Methods Length: 2
 - ▶ Compression Methods (2 methods)
 - Extensions Length: 111
 - ▶ Extension: ec_point_formats (len=4)
 - ▶ Extension: supported_groups (len=52)
 - ▶ Extension: session_ticket (len=0)
 - ▶ Extension: signature_algorithms (len=34)
 - ▶ Extension: heartbeat (len=1)

- ▼ Transport Layer Security
 - ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 161
 - ▼ Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 157
 - Version: TLS 1.2 (0x0303)
 - ▶ Random: 52362c1012cf23628256e745e903cea696e9f62a60ba0ae8...
 - Session ID Length: 0
 - Cipher Suites Length: 4
 - ▶ Cipher Suites (2 suites)
 - Compression Methods Length: 2
 - ▶ Compression Methods (2 methods)
 - Extensions Length: 111
 - ▶ Extension: ec_point_formats (len=4)
 - ▶ Extension: supported_groups (len=52)
 - ▶ Extension: session_ticket (len=0)
 - ▶ Extension: signature_algorithms (len=34)
 - ▶ Extension: heartbeat (len=1)

- ▼ Transport Layer Security
 - ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 161
 - ▼ Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 157
 - Version: TLS 1.2 (0x0303)
 - ▶ Random: 52362c1012cf23628256e745e903cea696e9f62a60ba0ae8...
 - Session ID Length: 0
 - Cipher Suites Length: 4
 - ▶ Cipher Suites (2 suites)
 - Compression Methods Length: 2
 - ▶ Compression Methods (2 methods)
 - Extensions Length: 111
 - ▶ Extension: ec_point_formats (len=4)
 - ▶ Extension: supported_groups (len=52)
 - ▶ Extension: session_ticket (len=0)
 - ▶ Extension: signature_algorithms (len=34)
 - ▶ Extension: heartbeat (len=1)

- ▼ Transport Layer Security
 - ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 161
 - ▼ Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 157
 - Version: TLS 1.2 (0x0303)
 - ▶ Random: 52362c1012cf23628256e745e903cea696e9f62a60ba0ae8...
 - Session ID Length: 0
 - Cipher Suites Length: 4
 - ▶ Cipher Suites (2 suites)
 - Compression Methods Length: 2
 - ▶ Compression Methods (2 methods)
 - Extensions Length: 111
 - ▶ Extension: ec_point_formats (len=4)
 - ▶ Extension: supported_groups (len=52)
 - ▶ Extension: session_ticket (len=0)
 - ▶ Extension: signature_algorithms (len=34)
 - ▶ Extension: heartbeat (len=1)

- ▼ Transport Layer Security
 - ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 161
 - ▼ Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 157
 - Version: TLS 1.2 (0x0303)
 - ▶ Random: 52362c1012cf23628256e745e903cea696e9f62a60ba0ae8...
 - Session ID Length: 0
 - Cipher Suites Length: 4
 - ▼ Cipher Suites (2 suites)
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 - Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
 - Compression Methods Length: 2
 - ▶ Compression Methods (2 methods)
 - Extensions Length: 111
 - ▶ Extension: ec_point_formats (len=4)
 - ▶ Extension: supported_groups (len=52)
 - ▶ Extension: session_ticket (len=0)
 - ▶ Extension: signature_algorithms (len=34)
 - ▶ Extension: heartbeat (len=1)

- ▼ Transport Layer Security
 - ▼ TLSv1.2 Record Layer: Handshake Protocol: **Server Hello**
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 66
 - ▼ Handshake Protocol: Server Hello
 - Handshake Type: Server Hello (2)
 - Length: 62
 - Version: TLS 1.2 (0x0303)**
 - ▶ Random: 52362c10a2665e323a2adb4b9da0c10d4a8823719272f8b4...
 - Session ID Length: 0
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)**
 - Compression Method: DEFLATE (1)
 - Extensions Length: 22
 - ▶ Extension: renegotiation_info (len=1)
 - ▶ Extension: ec_point_formats (len=4)
 - ▶ Extension: session_ticket (len=0)
 - ▶ Extension: heartbeat (len=1)

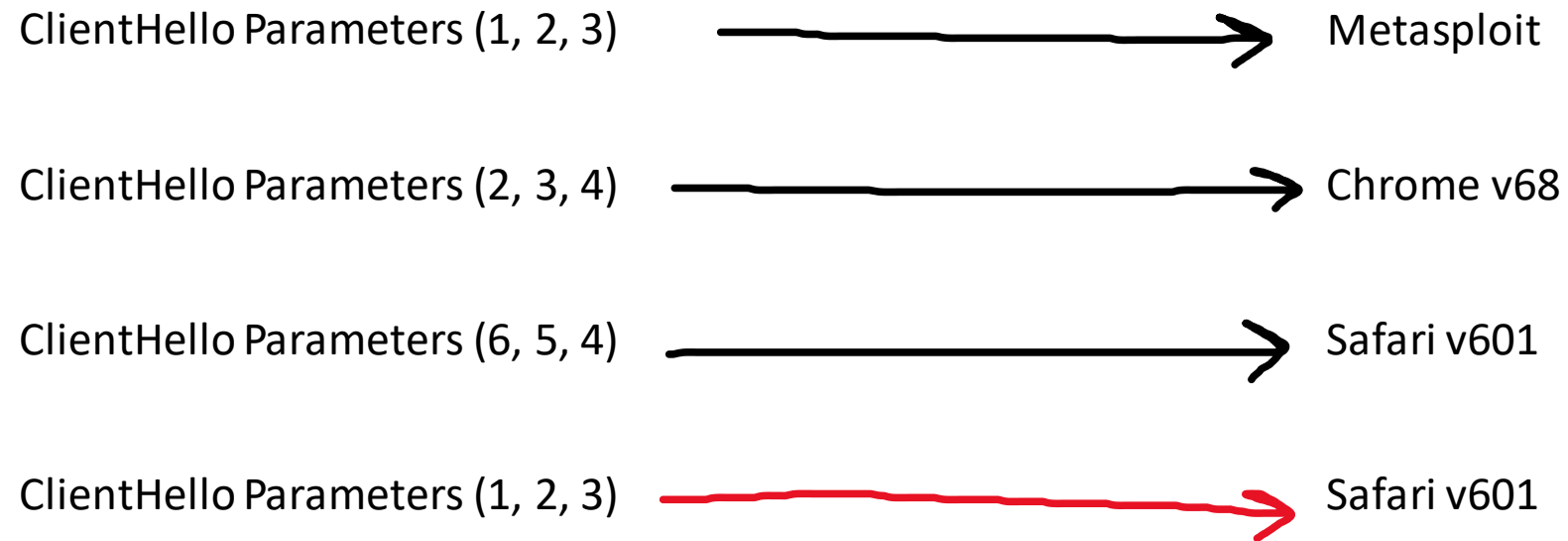
- ▼ Transport Layer Security
 - ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 161
 - ▼ Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 157
 - Version: TLS 1.2 (0x0303)
 - ▶ Random: 52362c1012cf23628256e745e903cea696e9f62a60ba0ae8...
 - Session ID Length: 0
 - Cipher Suites Length: 4
 - ▼ Cipher Suites (2 suites)
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 - Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
 - Compression Methods Length: 2
 - ▶ Compression Methods (2 methods)
 - Extensions Length: 111
 - ▶ Extension: ec_point_formats (len=4)
 - ▶ Extension: supported_groups (len=52)
 - ▶ Extension: session_ticket (len=0)
 - ▶ Extension: signature_algorithms (len=34)
 - ▶ Extension: heartbeat (len=1)

(ClientHello Parameters, User-Agent)

JA3 Parameters

- SSLVersion
- Cipher
- SSL Extension
- Elliptic Curve
- Elliptic CurvePointFormat

```
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 161
    ▼ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 157
      Version: TLS 1.2 (0x0303)
      Random: 52362c10a4530e7bcee0704c9dce137017972c1bbeaa8143...
      Session ID Length: 0
      Cipher Suites Length: 4
      ▼ Cipher Suites (2 suites)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
        Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
      Compression Methods Length: 2
      ► Compression Methods (2 methods)
      Extensions Length: 111
      ▼ Extension: ec_point_formats (len=4)
        Type: ec_point_formats (11)
        Length: 4
        EC point formats Length: 3
        ▼ Elliptic curves point formats (3)
          EC point format: uncompressed (0)
          EC point format: ansiX962_compressed_prime (1)
          EC point format: ansiX962_compressed_char2 (2)
      ▼ Extension: supported_groups (len=52)
```



769,47-53-5-10-49161-49162-49171-49172-50-56-19-4,0-10-11,23-24-25,0



060d8190af2b286011c49d9b1864e488

JA3Transport

<https://github.com/CUCyber/ja3transport>



CU CYBER



```
type RoundTripper interface {  
    RoundTrip(*Request) (*Response, error)  
}
```




```
tr := &http.Transport{  
    MaxIdleConns:    10,  
    IdleConnTimeout: 30 * time.Second,  
    DisableCompression: true,  
}  
client := &http.Client{Transport: tr}  
resp, err := client.Get("https://example.com")
```

Refraction.Networking



<https://refraction.networking>

[refraction-networking/utls](https://refraction.networking/utls)



```
tr, _ := ja3transport.NewTransport("771-61-60-53,0-23-15,29,23,24,0")  
client := &http.Client{Transport: tr}  
client.Get("https://ja3er.com/json")
```

13-21-28-46

Want:

- 13
- 21
- 28
- 46

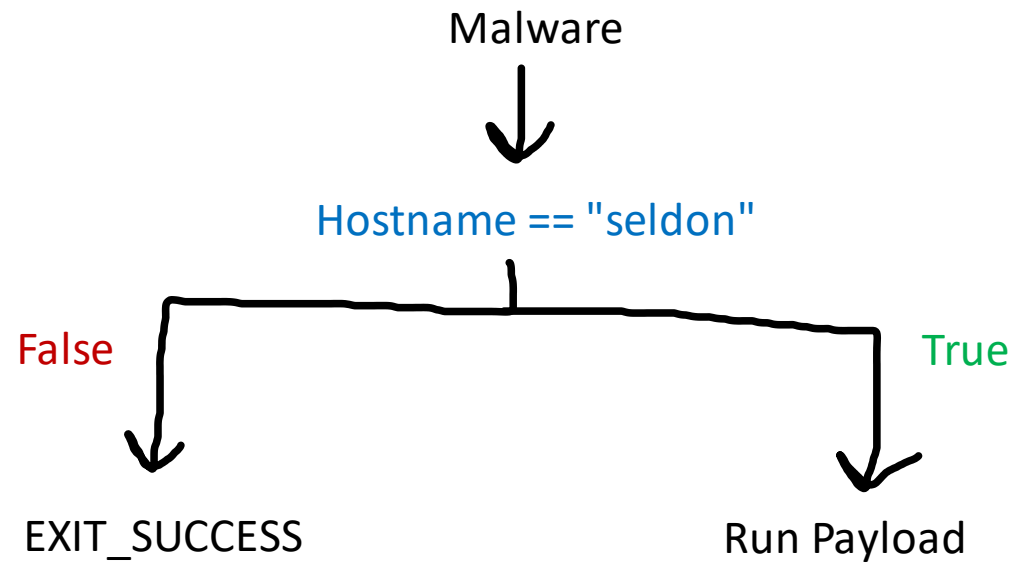
crypto/tls implements

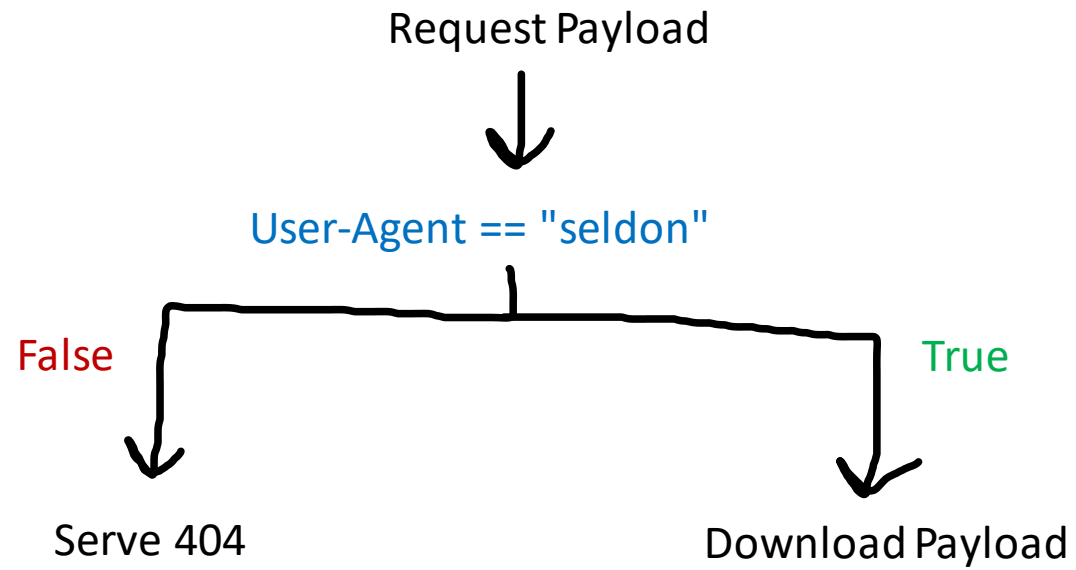
- 13
- 21
- 28

Satellite

<https://github.com/t94j0/satellite>









/var/www/html/payload.exe.info



- **authorized_useragents:**
 - Mozilla/5.0 (Android 4.4; Mobile; rv:41.0) Gecko/41.0 Firefox/41.0
- **blacklist_iprange:**
 - 123.123.123.123
 - 40.41.42.1/24



```
authorized_useragents:  
  - "*Mozilla*"br/>on_failure:  
  redirect: https://google.com
```



```
authorized_useragents:  
  - "*Mozilla*"br/>on_failure:  
  render: /404.html
```

Satellite Options

- serve
- {authorized,blacklist}_useragents
- {authorized,blacklist}_iprange
- {authorized,blacklist}_headers
- {authorized,blacklist}_countries
- credential_capture
- proxy



```
# /etc/satellite/conditions/plooppoint_ip.yml
```

```
blacklist_iprange:
```

- 127.0.0.1
- 127.0.0.2

```
# /etc/satellite/conditions/google.yml
```

```
blacklist_useragents:
```

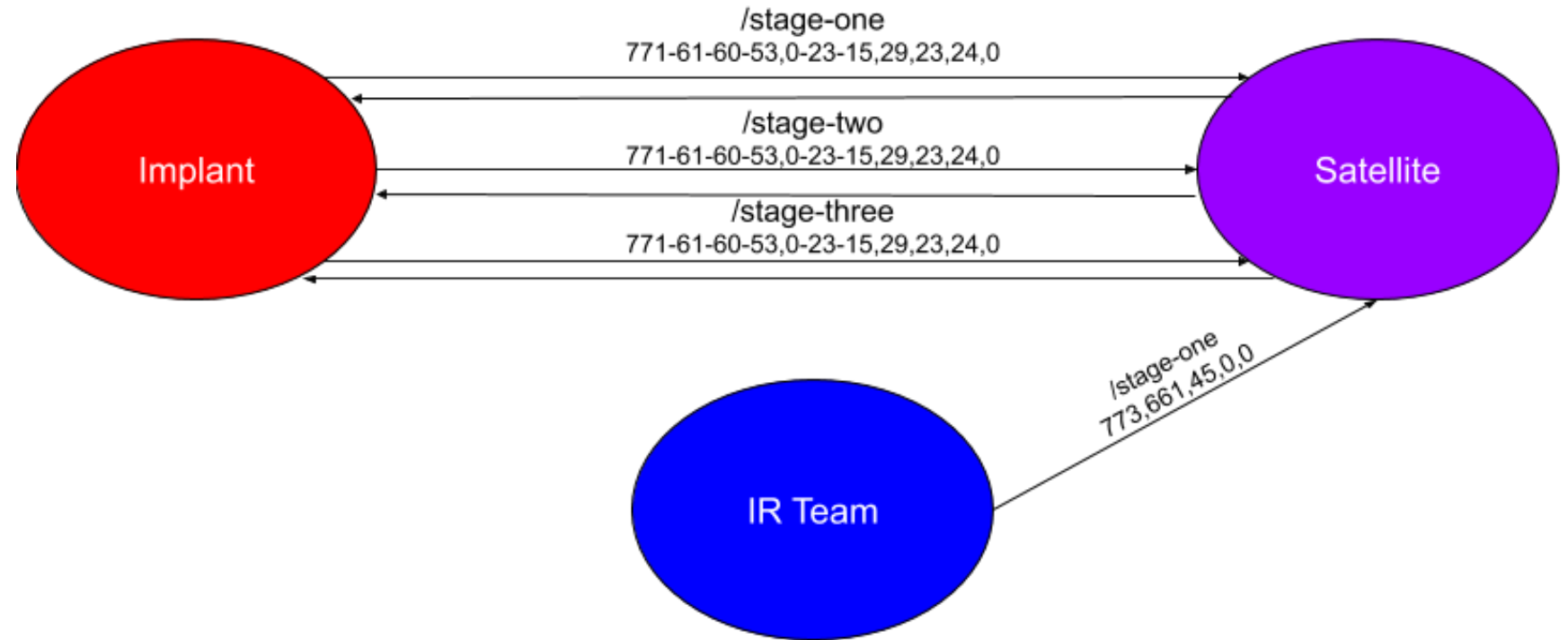
- Googlebot-Image/1.0
- Googlebot-News

Most Importantly...

- {authorized,blacklist}_ja3

Dynamic C2 with Satellite + JA3Transport

<https://bit.ly/3mX7SB5>

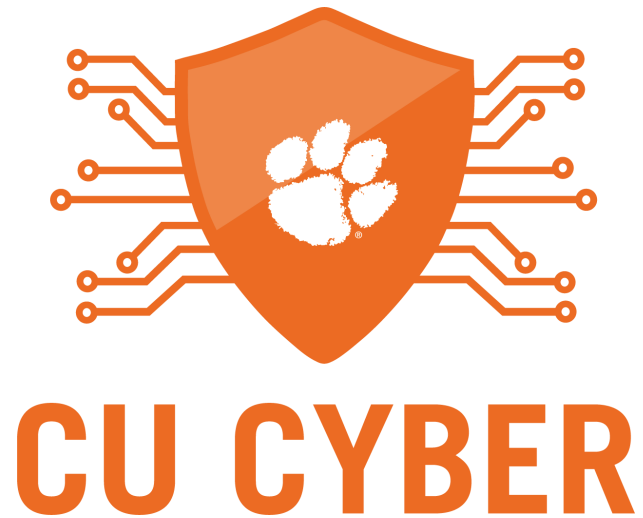


In the Future

- Compiler fork
- JA3 outbound proxy signature
- URI globbing for proxying
- Payload templates for HTML smuggling
- Authentication

Conclusion

<https://github.com/CUCyber/ja3transport>



<https://github.com/t94j0/satellite>



Call-to-Action

01

Make JA3 spoofing
libraries for other
languages

02

If you're using
Go, use
JA3Transport!

03

Try out Satellite



www.specterops.io



[@specterops](https://twitter.com/specterops)



info@specterops.io