

A complex network graph serves as the background, consisting of numerous small, dense clusters of blue and red dots connected by thin grey lines. A few larger, more prominent clusters are highlighted with thicker grey outlines. One such cluster is located at the bottom center, containing a large red core surrounded by blue and red nodes.

Profiling and Clustering Internet-Wide Scans with fatt.

Adel Karimi

\$whoami

0x4d31

- Lead Security Engineer, Salesforce 
- Honeynet Project
- Co-developer of HASSH profiling method &
a couple more open-source projects
 - <https://github.com/0x4D31>



Outline

- Background: Fingerprinting
 - SSL/TLS, SSH, RDP, HTTP, QUIC?
- Monitoring internet-wide scans
- Introducing FATT /fingerprintAllTheThings
- Observations
 - SSL/TLS
 - RDP
 - SSH

Could we use
Network Metadata & Fingerprints to
profile the attackers,

Could we use
Network Metadata & Fingerprints to
identify their tools,

Could we use
Network Metadata & Fingerprints to
discover new/hidden connections,

Could we use
Network Metadata & Fingerprints to
possibly **detect new evasion methods!?**

Background

Fingerprinting

OS Fingerprinting

httpprint

JA3

Browser Fingerprinting

fingerprinTLS

SSL/TLS Fingerprinting

p0f

Application Fingerprinting

HASSH

sslhaf



Cryptographic protocols need to
negotiate some parameters in

clear-text

TLS Client/Server Fingerprinting

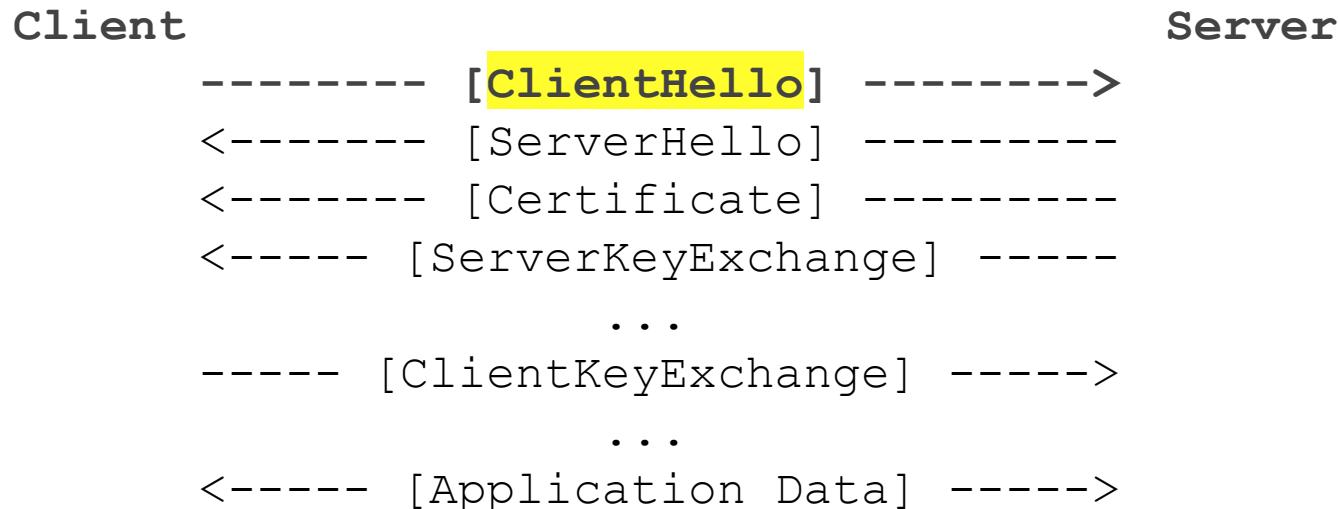
using client/server Hello messages

▼ Transport Layer Security
 ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 Content Type: Handshake (22)
 Version: TLS 1.0 (0x0301)
 Length: 329
 ▼ Handshake Protocol: Client Hello
 Handshake Type: Client Hello (1)
 Length: 325
 Version: TLS 1.2 (0x0303)
 ► Random: 8bd177cdf0d6c9ed5e3186125abd35f5a023e3ce8a1fa512...
 Session ID Length: 0
 Cipher Suites Length: 148
 ▼ Cipher Suites (74 suites)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc14)
 Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc13)
 Cipher Suite: TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc15)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
 Cipher Suite: TLS_DH_DSS_WITH_AES_256_GCM_SHA384 (0x00a5)
 Cipher Suite: TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3)
 Cipher Suite: TLS_DH_RSA_WITH_AES_256_GCM_SHA384 (0x00a1)
 Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
 Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)

0000	86 51 a4 84 a5 e5 cc e1	7f a8 17 f0 08 00 45 00	·Q..... E
0010	01 82 a4 92 40 00 35 06	c0 4e d9 b6 8f 61 45 37@·5· N · aE7
0020	31 46 a0 4b 01 bb 81 39	32 e7 b8 64 f6 46 80 18	1F·K· · 9 2· d·F· ..
0030	00 e5 62 e6 00 00 01 01	08 0a 04 4c 96 88 25 f6	·b..... ·L·%· ..
0040	13 c3 16 03 01 01 49 01	00 01 45 03 03 8b d1 77I· .E· ..w
0050	cd f0 d6 c9 ed 5e 31 86	12 5a bd 35 f5 a0 23 e3^1· .Z·5·#· ..
0060	ce 8a 1f a5 12 6c 18 8f	fa ff 4a 8f c7 00 00 94l· .J· ..
0070	cc 14 cc 13 cc 15 c0 30	c0 2c c0 28 c0 24 c0 140· ,·(·\$..
0080	c0 0a 00 a5 00 a3 00 a1	00 9f 00 6b 00 6a 00 69k·j·i
0090	00 68 00 39 00 38 00 37	00 36 c0 32 c0 2e c0 2a	·h·9·8·7· .6·2·..*
00a0	c0 26 c0 0f c0 05 00 9d	00 3d 00 35 00 95 c0 2f	&..... =·5·// ..
00b0	c0 2b c0 27 c0 23 c0 13	c0 09 00 a4 00 a2 00 a0	++·'·#..
00c0	00 9e 00 67 00 40 00 3f	00 3e 00 33 00 32 00 31	..g·@·?· .>·3·2·1
00d0	00 30 c0 31 c0 2d c0 29	c0 25 c0 0e c0 04 00 9c	·0·1·..) .%. . . .
00e0	00 3c 00 2f 00 94 00 9a	00 99 00 98 00 97 00 96	<·/.....
00f0	00 07 c0 11 c0 07 00 66	c0 0c c0 02 00 05 00 04f

SSL/TLS Handshake

- Message Flow for a SSL/TLS Handshake



SSL/TLS ClientHello

```
struct {
    ProtocolVersion client_version;
    Random random;
    SessionID session_id;
    CipherSuite cipher_suites<2..2^16-2>;
    CompressionMethod compression_methods<1..2^8-1>;
    select (extensions_present) {
        case false:
            struct {};
        case true:
            Extension extensions<0..2^16-1>;
    };
} ClientHello;
```

SSL/TLS ClientHello

```
struct {
    ProtocolVersion client_version;
    Random random;
    SessionID session_id;
    CipherSuite cipher_suites<2..2^16-2>;
    CompressionMethod compression_methods<1..2^8-1>;
    select (extensions_present) {
        case false:
            struct {};
        case true:
            Extension extensions<0..2^16-1>;
    };
} ClientHello;
```

The **cipher suite list** in the ClientHello message, contains the combinations of cryptographic algorithms supported by the client
in order of the client's preference

TLS Fingerprinting /mod_sslhaf

- An Apache module that passively monitors initial SSL handshakes to extract and log SSL client capabilities

```
Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.11) Gecko/2009061118 Firefox/3.0
Handshake: h3
Protocol: 03.01

TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA (0x87)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x38)
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA (0x44)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)
TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x32)
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)
TLS_RSA_WITH_RC4_128_MD5 (0x04)
TLS_RSA_WITH_RC4_128_SHA (0x05)
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x13)
SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA (0xffff)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)
```

TLS Fingerprinting /mod_sslhaf

- An Apache module that passively monitors initial SSL handshakes to extract and log SSL client capabilities

```
Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.11) Gecko/2009061118 Firefox/3.0  
Handshake: h3  
Protocol: 03.01
```

“Cross-checking the **supported cipher suites** with the HTTP client identity offered in the User-Agent header may help uncover some automated attack tools that masquerade themselves as browsers.”

```
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)  
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x13)  
SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA (0xffff)  
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x0a)
```

TLS Fingerprinting /pof

- Unofficial SSL fingerprinting module for p0f

```
label = s:!Firefox:11 (TOR)
sys   = Windows,@unix
; Lack of a single extension (SessionTicket TLS) is not a very strong signal.
sig   = 3.1:ff,c00a,c014,88,87,39,38,*,c003,feff,a:?0,a,b:

label = s:!Firefox:14 or newer
sys   = Windows,@unix
sig   = 3.1:ff,c00a,c014,88,87,39,38,*,c003,feff,a:?0,a,b,23,3374:

; with TLS switched off
label = s:!Firefox:3.6.X or newer
sys   = Windows,@unix
sig   = 3.0:ff,88,87,39,38,84,35,45,44,33,32,96,41,4,5,2f,16,13,feff,a::
```

TLS Fingerprinting /FingerprinTLS

- A set of tools to enable the matching, creation, and export of TLS Fingerprints.

record_tls_version, tls_version, ciphersuite_length, ciphersuite, compression_length, compression, e_curves, sig_alg, ec_point_fmt

- ```
{"id": 0, "desc": "AppleWebKit/533.1 (KHTML like Gecko) Version/4.0 Mobile Safari/533.1", "record_tls_version": "0x0301", "tls_version": "0x0301", "ciphersuite_length": "0x0020", "ciphersuite": "0x0004 0x0005 0x002F 0x0033 0x0032 0x000A 0x0016 0x0013 0x0009 0x0015 0x0012 0x0003 0x0008 0x0014 0x0011 0x00FF", "compression_length": "1", "compression": "0x00", "extensions": ""}
```

# TLS Fingerprinting /JA3

- A method for creating SSL/TLS client fingerprints that are easy to produce and can be easily shared.

**tls\_version, ciphersuites, extensions, elliptic\_curves, ec\_point\_format**

- Example:
  - JA3 string: 769,47-53-5-10-49161-49162-49171-49172-50-56-19-4,0-10-11,23-24-25,0
  - JA3 (md5 hash): ada70206e40642a3e4461f35503241d5

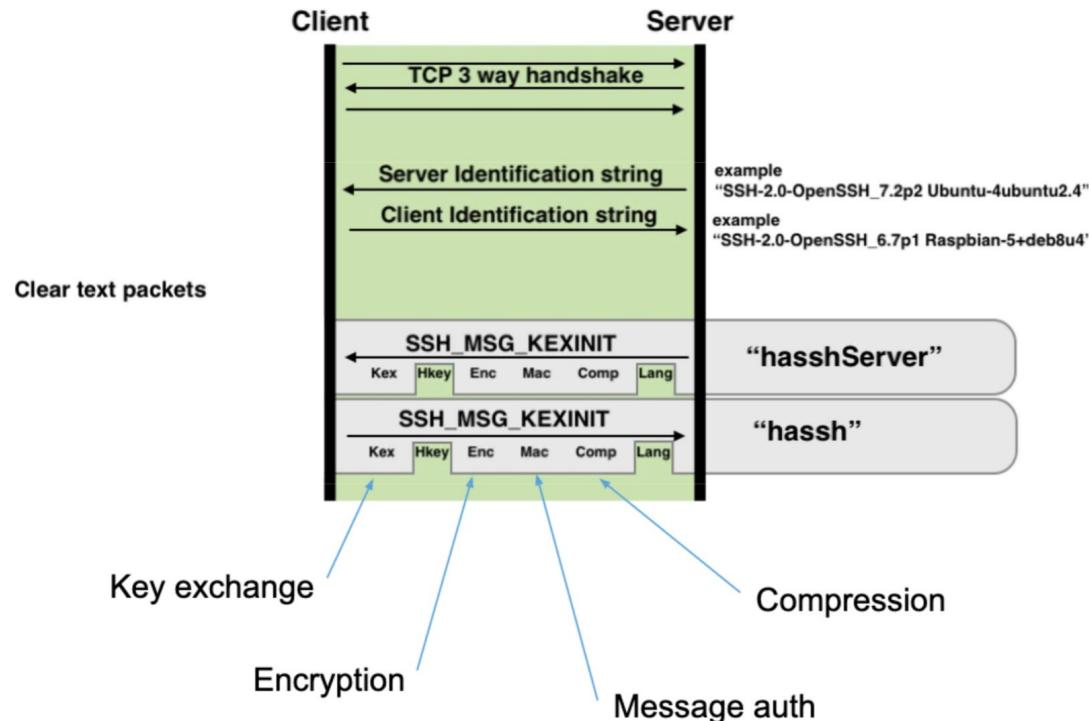
# SSH Client/Server Fingerprinting

using `SSH_MSG_KEXINIT` messages

SSH Protocol  
  ▼ SSH Version 2  
    Packet Length: 1388  
    Padding Length: 4  
  ▼ Key Exchange  
    Message Code: Key Exchange Init (20)  
    ▼ Algorithms  
      Cookie: 493c1ff88f5c28692341c15022837f1b  
      kex\_algorithms length: 269  
      kex\_algorithms string [truncated]: curve25519-sha256,curve25519-sha256-ecdh-sha256-sha256  
      server\_host\_key\_algorithms length: 358  
      server\_host\_key\_algorithms string [truncated]: ecdsa-sha2-nistp256-cert-v02@openssh.com,ecdh-sha2-nistp256-cert-v02@openssh.com,ecdh-sha2-nistp256,ecdsa-sha2-nistp256  
      encryption\_algorithms\_client\_to\_server length: 108  
      encryption\_algorithms\_client\_to\_server string: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr  
      encryption\_algorithms\_server\_to\_client length: 108  
      encryption\_algorithms\_server\_to\_client string: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr  
      mac\_algorithms\_client\_to\_server length: 213  
      mac\_algorithms\_client\_to\_server string [truncated]: umac-64-etm@openssh.com  
      mac\_algorithms\_server\_to\_client length: 213  
      mac\_algorithms\_server\_to\_client string [truncated]: umac-64-etm@openssh.com  
      compression\_algorithms\_client\_to\_server length: 26  
      compression\_algorithms\_client\_to\_server string: none,zlib@openssh.com  
      compression\_algorithms\_server\_to\_client length: 26  
      compression\_algorithms\_server\_to\_client string: none,zlib@openssh.com  
      languages\_client\_to\_server length: 0  
      languages\_client\_to\_server string: [Empty]  
      languages\_server\_to\_client length: 0  
      languages\_server\_to\_client string: [Empty]  
      First KEX Packet Follows: 0  
      Reserved: 00000000  
      Padding String: 00000000

```
0000 00 00 05 6c 04 14 49 3c 1f f8 8f 5c 28 69 23 41 ···l.I< ···\(\i#A
0010 c1 50 22 83 7f 1b 00 00 01 0d 63 75 72 76 65 32 .P"..... ··curve2
0020 35 35 31 39 2d 73 68 61 32 35 36 2c 63 75 72 76 5519-sha 256,curv
0030 65 32 35 35 31 39 2d 73 68 61 32 35 36 40 6c 69 e25519-s ha256@li
0040 62 73 73 68 2e 6f 72 67 2c 65 63 64 68 2d 73 68 bssh.org ,ecdh-sh
0050 61 32 2d 6e 69 73 74 70 32 35 36 2c 65 63 64 68 a2-nistp 256,ecdh
0060 2d 73 68 61 32 2d 6e 69 73 74 70 33 38 34 2c 65 -sha2-ni stp384,e
0070 63 64 68 2d 73 68 61 32 2d 6e 69 73 74 70 35 32 cdh-sha2 -nistp52
0080 31 2c 64 69 66 66 69 65 2d 68 65 6c 6c 6d 61 6e 1,diffie -hellman
0090 2d 67 72 6f 75 70 2d 65 78 63 68 61 6e 67 65 2d -group-e xchange-
```

# HASSH Profiling Method



# HASSH - examples

- hassh(**Ncrack**) = 55a77ae9728654f1d4240a29287dc296
- hassh(**CobaltStrike\_SSH-client**) = a7a87fbe86774c2e40cc4a7ea2ab1b3c
- hassh(**Cowrie**) = a0fd4bc0e72b4b21232a486825b6742
- hasshGen:

| image  | imageVersion | sshClient | sshClientVersion | clientIdentificationString | hassh                            |
|--------|--------------|-----------|------------------|----------------------------|----------------------------------|
| debian | sid-slim     | dropbear  | 2018.76-4        | SSH-2.0-dropbear_2018.76   | e22efe3cde8b396b874c3f13fdb6c61a |
| debian | buster-slim  | dropbear  | 2018.76-4        | SSH-2.0-dropbear_2018.76   | e22efe3cde8b396b874c3f13fdb6c61a |
| debian | stretch-slim | dropbear  | 2016.74-5        | SSH-2.0-dropbear_2016.74   | 7742887e2a57712bdb91a772093f54ce |
| debian | jessie-slim  | dropbear  | 2014.65-1+deb8u2 | SSH-2.0-dropbear_2014.65   | ad00edb0c2a031d9884826ba7b7ba41e |

# RDP, a hot topic these days..

CVE-2019-0708 //blueKeep

# RDP Fingerprinting

using ClientHello & ClientInfo messages

```
▼ Remote Desktop Protocol
 ▼ ClientData
 ▼ clientCoreData
 headerType: clientCoreData (0xc001)
 headerLength: 212
 versionMajor: 4
 versionMinor: 8
 desktopWidth: 1280
 desktopHeight: 800
 colorDepth: 8 bits-per-pixel (bpp) (0xca01)
 SASSequence: 43523
 keyboardLayout: 2057
 clientBuild: 2600
 clientName: EMP-LAP-0014
 keyboardType: IBM enhanced (101-key or 102-key) keyboard (4)
 keyboardSubType: 0
 keyboardFunctionKey: 12
 imeFileName: 00...
 postBeta2ColorDepth: 8 bits-per-pixel (bpp) (0xca01)
 clientProductId: 1
 serialNumber: 0
 highColorDepth: 16-bit 565 RGB mask (0x0010)
 supportedColorDepths: 0x0007
 earlyCapabilityFlags: 1
 clientDigProductId: 76487-OEM-0011903-00107
 connectionType: Unknown (0)
 padloctet: 0x00
 ▶ clientClusterData
 ▼ clientSecurityData
 headerType: clientSecurityData (0xc002)
 headerLength: 12
 encryptionMethods: 01000000
 extEncryptionMethods: 00000000
 ▶ clientNetworkData
```

|      |                         |                         |                   |   |
|------|-------------------------|-------------------------|-------------------|---|
| 0000 | 86 51 a4 84 a5 e5 cc e1 | 7f a8 1b f0 08 00 45 00 | Q . . . . . . . . | E |
| 0010 | 01 d0 91 19 40 00 35 06 | 4c fc c4 34 2b 61 45 37 | ...@ 5 L . 4+aE7  |   |
| 0020 | 31 46 d5 3e 0d 3d 1c 48 | 78 9f 99 04 6d 16 80 18 | 1F->.=H x .m . .  |   |

# RDP Negotiation Request

- requestedProtocols

|   |          |             |       |              |       |     |                                                     |
|---|----------|-------------|-------|--------------|-------|-----|-----------------------------------------------------|
| 4 | 0.274459 | 10.127.1... | 53073 | 3.89.47.1... | 3389  | RDP | Negotiate Request                                   |
| 5 | 0.550412 | 3.89.47...  | 3389  | 10.127.18... | 53073 | TCP | 3389 → 53073 [ACK] Seq=1 Ack=20 Win=65536 Len=0 TS\ |
| 6 | 0.550465 | 3.89.47...  | 3389  | 10.127.18... | 53073 | RDP | Negotiate Response                                  |

# RDP Security Modes

- Enhanced RDP Security
  - TLS 1.0 / TLS 1.1 / TLS 1.2 / CredSSP / RDSTLS
  - **TLS → Can be fingerprinted with JA3**
- Standard RDP Security
  - requestedProtocols=0x00000000
  - **NO TLS**

# RDP Standard Security /ClientInfo

- **RDFP**; an experimental fingerprint for Standard RDP Security
  - Current composition (not perfect, but it works for my use-case):

md5(verMajor;verMinor;clusterFlags;encryptionMethods;extEncMethods;channelDef)

| 8  | 0.003577 | 172.16.1... | 39079 | 172.16.49... | 3389  | RDP  | ClientData                                  |  |
|----|----------|-------------|-------|--------------|-------|------|---------------------------------------------|--|
| 9  | 0.003676 | 172.16.4... | 3389  | 172.16.12... | 39079 | TCP  | 3389 → 39079 [ACK] Seq=20 Ack=502 Win=64240 |  |
| 10 | 0.004104 | 172.16.4... | 3389  | 172.16.12... | 39079 | RDP  | ServerData Encryption: 128-bit RC4 (Client) |  |
| 11 | 0.005352 | 172.16.1... | 39079 | 172.16.49... | 3389  | COTP | DT_TPDUL (0) EOT                            |  |

► Frame 8: 512 bytes on wire (4096 bits), 512 bytes captured (4096 bits)  
► Ethernet II, Src: Vmware\_35:84:c6 (00:50:56:35:84:c6), Dst: Vmware\_e6:24:31 (00:50:56:e6:24:31)  
► Internet Protocol Version 4, Src: 172.16.12.149, Dst: 172.16.49.130  
► Transmission Control Protocol, Src Port: 39079, Dst Port: 3389, Seq: 44, Ack: 20, Len: 458  
► TPKT, Version: 3, Length: 458  
► ISO 8073/X.224 COTP Connection-Oriented Transport Protocol  
► MULTIPONT-COMMUNICATION-SERVICE T.125  
► GENERIC-CONFERENCE-CONTROL T.124  
▼ Remote Desktop Protocol  
    ▼ ClientData  
        ► clientCoreData  
        ► clientClusterData  
        ▼ clientSecurityData  
            headerType: clientSecurityData (0xc002)  
            headerLength: 12  
            encryptionMethods: 03000000  
            extEncryptionMethods: 00000000  
        ► clientNetworkData

# HTTP

HTTP Fingerprinting

[net-square.com/httprint\\_paper.html](http://net-square.com/httprint_paper.html)

# QUICK

<https://github.com/0x4D31/quick>

# what else?

2019/05/11 05:42:10 192.168.1.9:56149 -> 172.217.167.74:443(  
Public Flags: d  
CID: b8142bd8c89f0e6e  
Version: Q043  
Packet Number: 1  
Message Authentication Hash: 924c2de3a9be804519ffa6e3  
Frame Type: a0  
Stream ID: 1  
Data Length: 1024  
Tag: CHLO  
Tag Number: 25  
SNI: "fonts.googleapis.com"  
UAID: "Chrome/74.0.3729.131 Intel Mac OS X 10\_14\_4"  
Tags in Order: ["PAD" "SNI" "STK" "VER" "CCS" "NONC" "AEAD" "UA"  
Tag Values: map[AEAD: AESG CCRT: 86c30bf78fd9372c67f8adc58015e3ff]

2019/05/11 05:42:10 192.168.1.9:58556 -> 172.217.25.174:443(  
Public Flags: d  
CID: e4fcac1c8ad38dc14  
Version: Q043  
Packet Number: 1  
Message Authentication Hash: 478ed5740d47dccc07b86b43  
Frame Type: a0  
Stream ID: 1  
Data Length: 1024  
Tag: CHLO  
Tag Number: 25  
SNI: "[www.youtube.com](http://www.youtube.com)"  
UAID: "Chrome/74.0.3729.131 Intel Mac OS X 10\_14\_4"  
Tags in Order: ["PAD" "SNI" "STK" "VER" "CCS" "NONC" "AEAD" "UA"  
Tag Values: map[AEAD: AESG CCRT: 2237aaad1bebaa6c67f8adc58015e3ff]

# Monitoring Internet-Wide Scans

# The Problem

- Honeypots: Limited network logging
  - General connection info and application-level data
  - No network metadata and handshake logging!

# Network Metadata

- Bro/Zeek
- Suricata
  - HTTP, DNS, TLS
- Tshark
- Netcap

## ssl.log | SSL handshakes

| FIELD                                | TYPE                         | DESCRIPTION                                                                         |
|--------------------------------------|------------------------------|-------------------------------------------------------------------------------------|
| ts                                   | time                         | Timestamp when SSL connection was established                                       |
| uid & id                             |                              | Underlying connection info > See https://www.wireshark.org/docs/man-pages/ssl.html  |
| version                              | string                       | SSL version that the server offered                                                 |
| cipher                               | string                       | SSL cipher suite that the server chose                                              |
| curve                                | string                       | Elliptic curve server chose if using ECDHE                                          |
| server_name                          | string                       | Value of Server Name Indicator SSL extension                                        |
| session_id                           | string                       | Session ID offered by client for session resumption                                 |
| resumed                              | bool                         | Flag that indicates the session was resumed                                         |
| last_alert                           | string                       | Last alert that was seen during the connection                                      |
| next_protocol                        | string                       | Next protocol server chose using application layer next protocol extension, if seen |
| established                          | bool                         | Was this connection established successfully?                                       |
| cert_chain <sup>1</sup>              | vector                       | Chain of certificates offered by server                                             |
| cert_chain_fuids <sup>1</sup>        | vector                       | File UIDs for certs in cert_chain                                                   |
| client_cert_chain <sup>1</sup>       | vector                       | Chain of certificates offered by client                                             |
| client_cert_chain_fuids <sup>1</sup> | vector                       | File UIDs for certs in client_cert_chain                                            |
| subject <sup>1</sup>                 | string                       | Subject of the X.509 cert offered by server                                         |
| issuer <sup>1</sup>                  | string                       | Subject of the signer of the server cert                                            |
| client_subject <sup>1</sup>          | string                       | Subject of the X.509 cert offered by client                                         |
| client_issuer <sup>1</sup>           | string                       | Subject of the signer of the client cert                                            |
| validation_status <sup>2</sup>       | string                       | Certificate validation result for this handshake                                    |
| ocsp_status <sup>2</sup>             | string                       | OCSP validation result for this handshake                                           |
| ocsp_response <sup>2</sup>           | string                       | OCSP response as a string                                                           |
| notary <sup>3</sup>                  | Cert<br>Notary::<br>Response | A response from the ICSI certificate notary                                         |

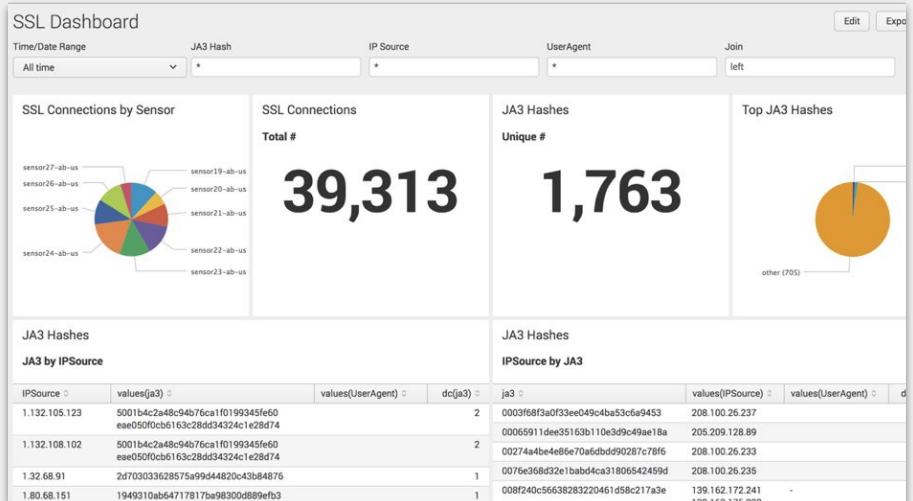
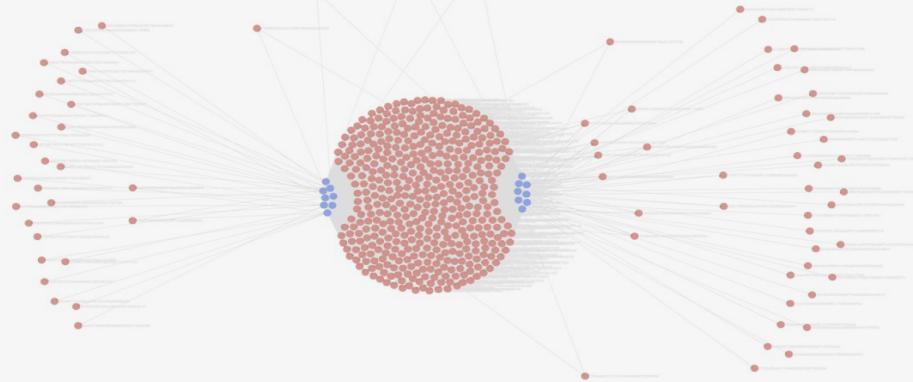


# honeyTLS

{Monitoring Internet-wide SSL/TLS scans}

- The first version of this research
- Monitoring tool: Bro + JA3 script
- Honeypot:
  - Nginx with open TLS ports
  - 443, 993, 995, 636, 614, 563, ...
- Splunk: access\_log join ssl.log

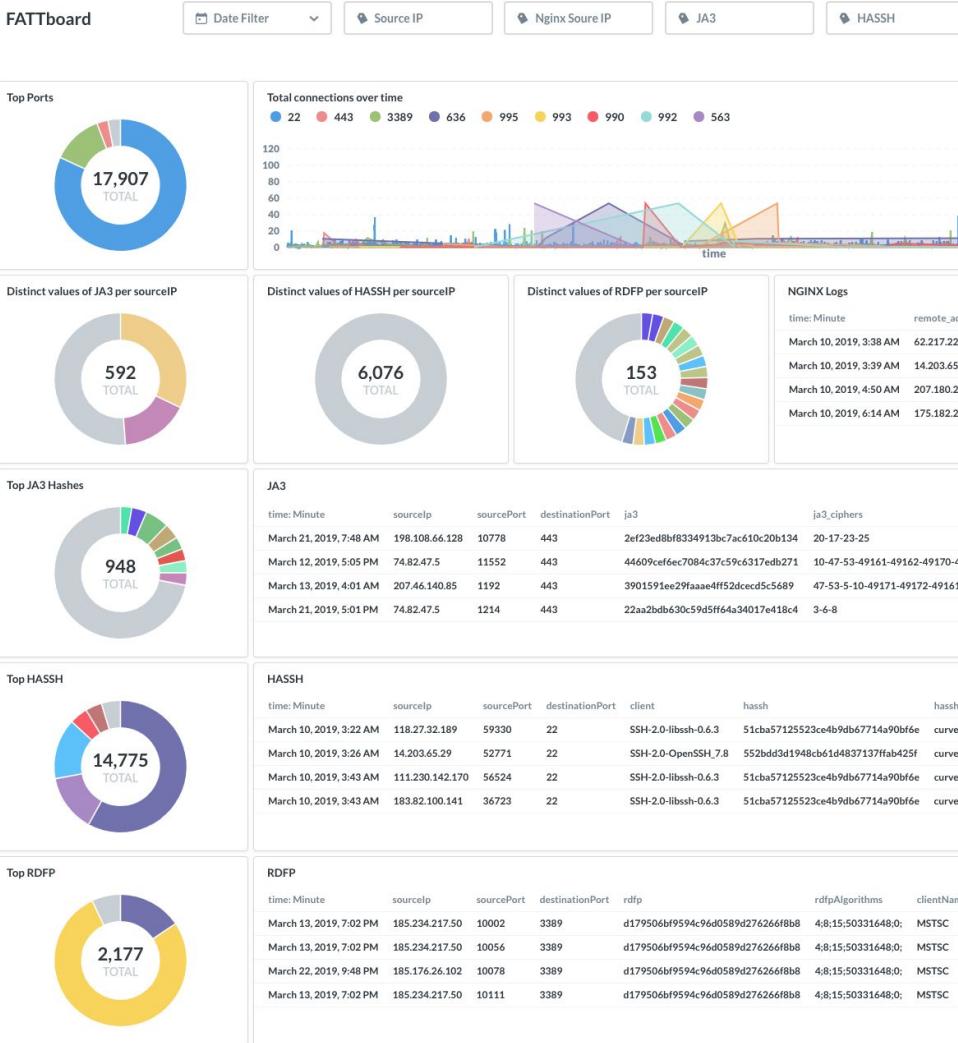
{..., ipSrc, ja3, ja3\_str, userAgent, request}



# FATT

## {Monitoring Internet-wide scans}

- Monitoring tool: **FATT (tshark)**
- Honeypot:
  - **Nginx** with open TLS and HTTP ports
  - **rDPy** for RDP
  - **Caddy** for QUIC
- Fluentd + Mongodb + Metabase



fatt.

fingerprint all the things!



66 61 74 74 2e  
fingerprint all the things!

- a pyshark based script for extracting **network metadata** and **fingerprints** from pcap files and live network traffic
- Supported protocols: TLS, SSH, RDP, HTTP, gQUIC
- Main use-case: monitoring honeypots, network forensics
- Easy to add new protocols
- Json output
- Downside: Performance

<https://github.com/0x4D31/fatt>



66 61 74 74 2e  
fingerprint all the things!

Terminal: Local × +

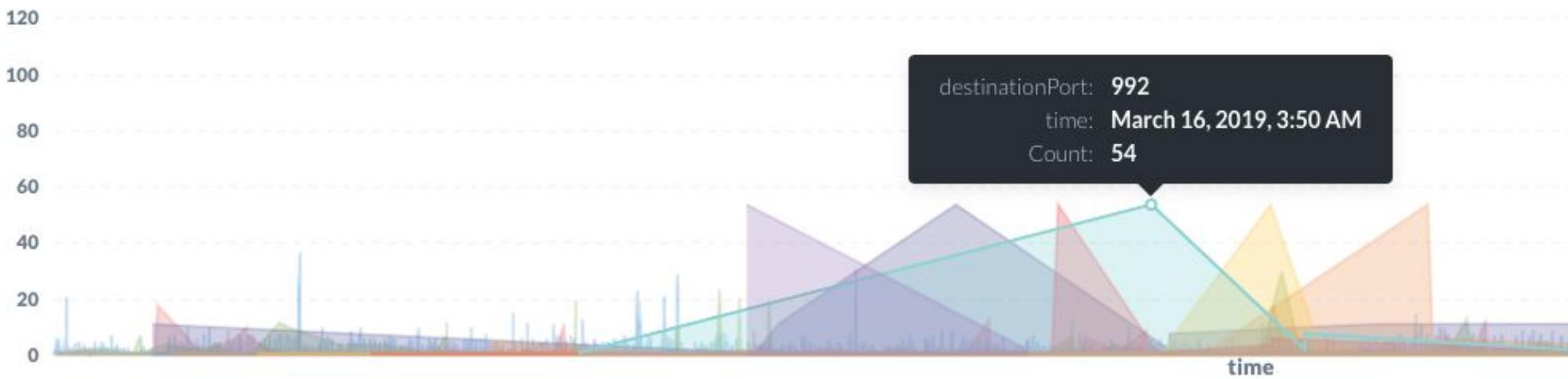
```
$ python3 fatt.py -i en0 -p
192.168.1.10:49599 -> 216.58.196.142:80 [HTTP] hash=d6662c018cd4169689ddf7c6c0f8ca1b userAgent="curl/7.54.0"
216.58.196.142:80 -> 192.168.1.10:49599 [HTTP] hash=c5241aca9a7c86f06f476592f5dda9a1 server=gws
13.237.44.5:22 -> 192.168.1.10:49603 [SSH] hasshS=3f0099d323fed5119bbfcc064478207 server=SSH-2.0-babeld-80573d3e
192.168.1.10:49603 -> 13.237.44.5:22 [SSH] hassh=ec7378c1a92f5a8dde7e8b7a1dddf33d1 client=SSH-2.0-OpenSSH_7.9
192.168.1.10:59661 -> 216.58.199.35:443 [QUIC] UAID="Chrome/74.0.3729.169 Intel Mac OS X 10_14_5" SNI=ssl.gstatic.com AEAD=AESG
192.168.1.10:49609 -> 93.184.216.34:443 [TLS] ja3=e6573e91e6eb777c0933c5b8f97f10cd serverName=example.com
93.184.216.34:443 -> 192.168.1.10:49609 [TLS] ja3s=ae53107a2e47ea20c72ac44821a728bf
192.168.1.10:49635 -> 192.168.1.3:80 [HTTP] hash=598c34a2838e82f9ec3175305f233b89 userAgent="Spotify/109600181 OSX/0 (MacBookPro
192.168.1.10:49645 -> 13.70.72.233:443 [TLS] ja3=4e30215bd4af6afe796e9ff893e7f3cd serverName=gate.hockeyapp.net
13.70.72.233:443 -> 192.168.1.10:49645 [TLS] ja3s=15381d64ba148f31a70eb87b53085230
192.168.1.10:49653 -> 192.168.1.3:80 [HTTP] hash=598c34a2838e82f9ec3175305f233b89 userAgent="Spotify/109600181 OSX/0 (MacBookPro
192.168.1.10:64046 -> 216.58.203.106:443 [QUIC] UAID="Chrome/74.0.3729.169 Intel Mac OS X 10_14_5" SNI=signaler-pa.clients6.google.com AEAD=AESG
192.168.1.10:54445 -> 172.217.25.142:443 [QUIC] UAID="Chrome/74.0.3729.169 Intel Mac OS X 10_14_5" SNI=clients6.google.com AEAD=AESG
192.168.1.10:54445 -> 172.217.25.142:443 [QUIC] UAID="Chrome/74.0.3729.169 Intel Mac OS X 10_14_5" SNI=clients6.google.com AEAD=AESG
^CExiting..
BYE o/
```

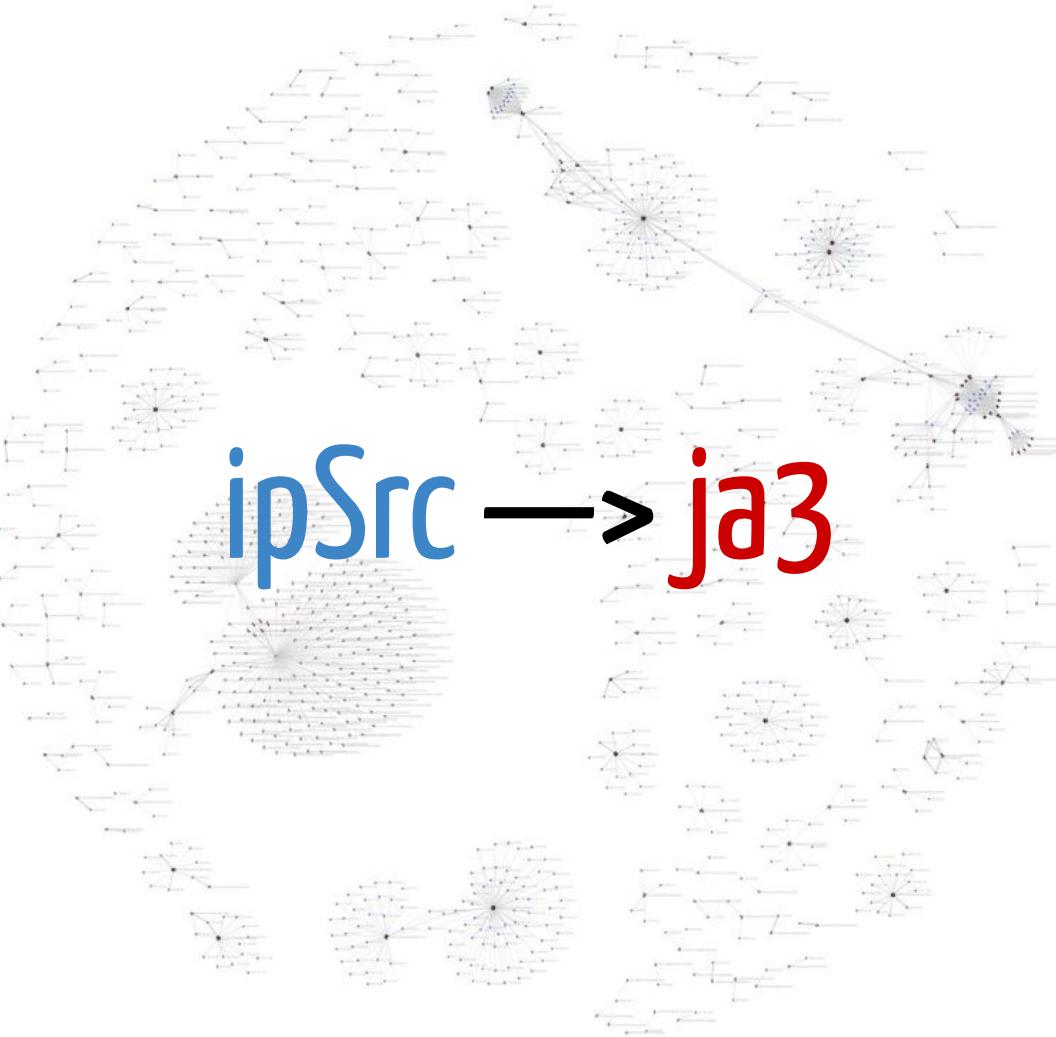
# Observations

## TLS

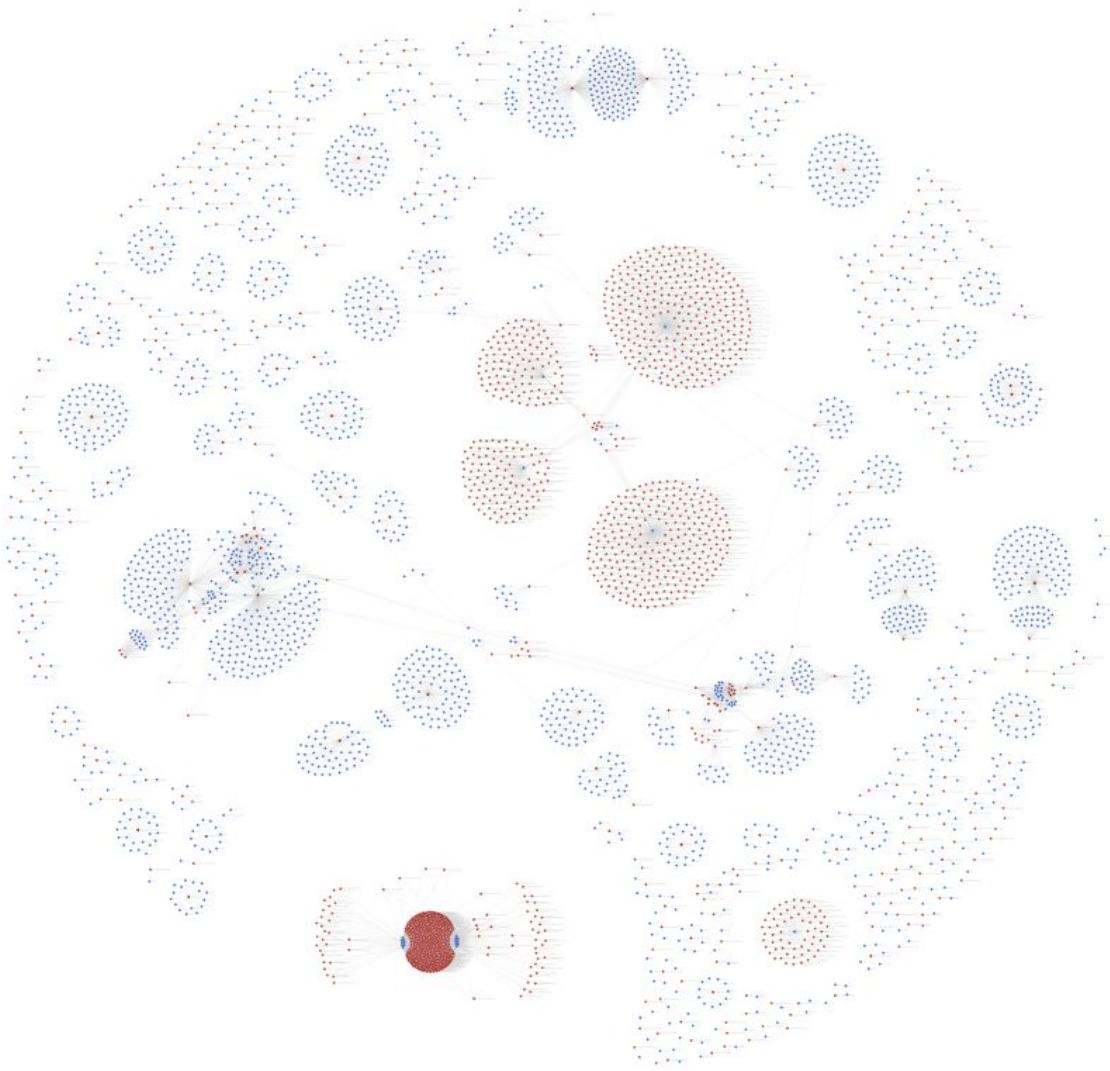
### Total connections over time

- 22 ● 443 ● 3389 ● 636 ● 995 ● 993 ● 990 ● 992 ● 563



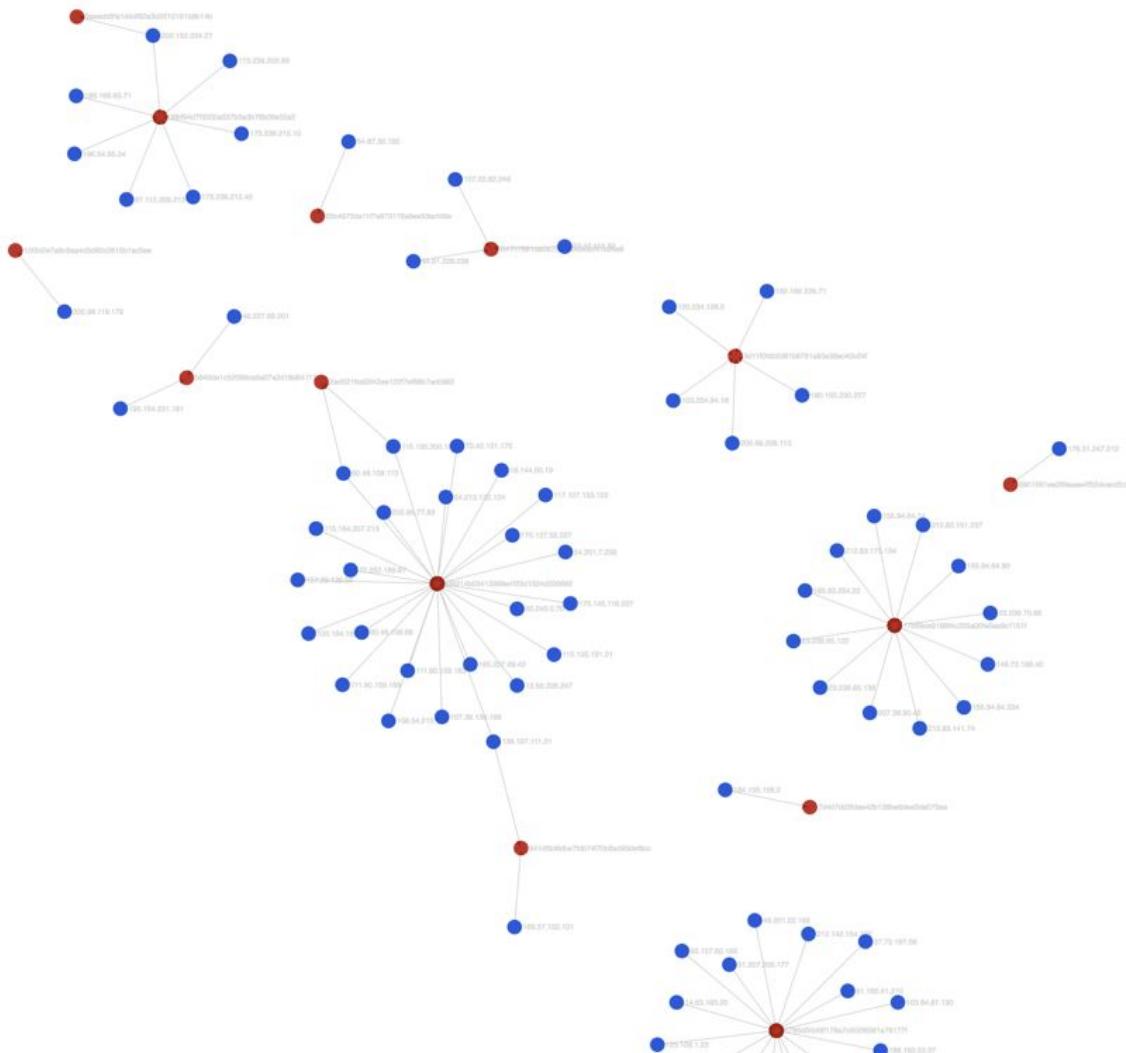


ipSrc → ja3



ipSrc → ja3

ipSrc → ja3



Observed some attempts to  
avoid SSL/TLS fingerprinting by  
randomizing the clientHello fields!

The first identified attempt: Dec 2017; Reported in Jul 2018!

<https://twitter.com/0x4d31/status/1017880884689584128>

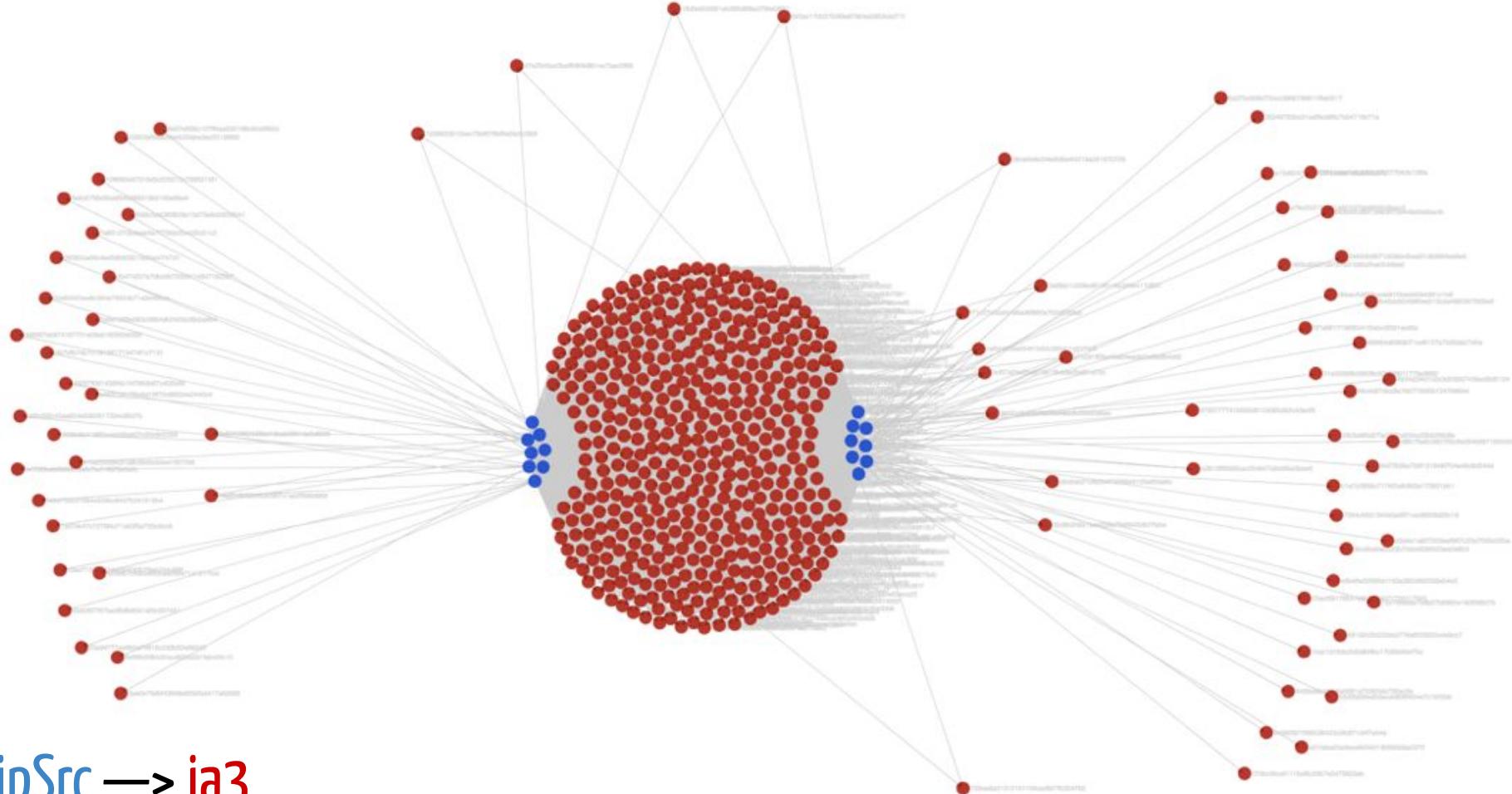
<https://twitter.com/4A4133/status/1133755095445852160>

one IP address → many JA3 values

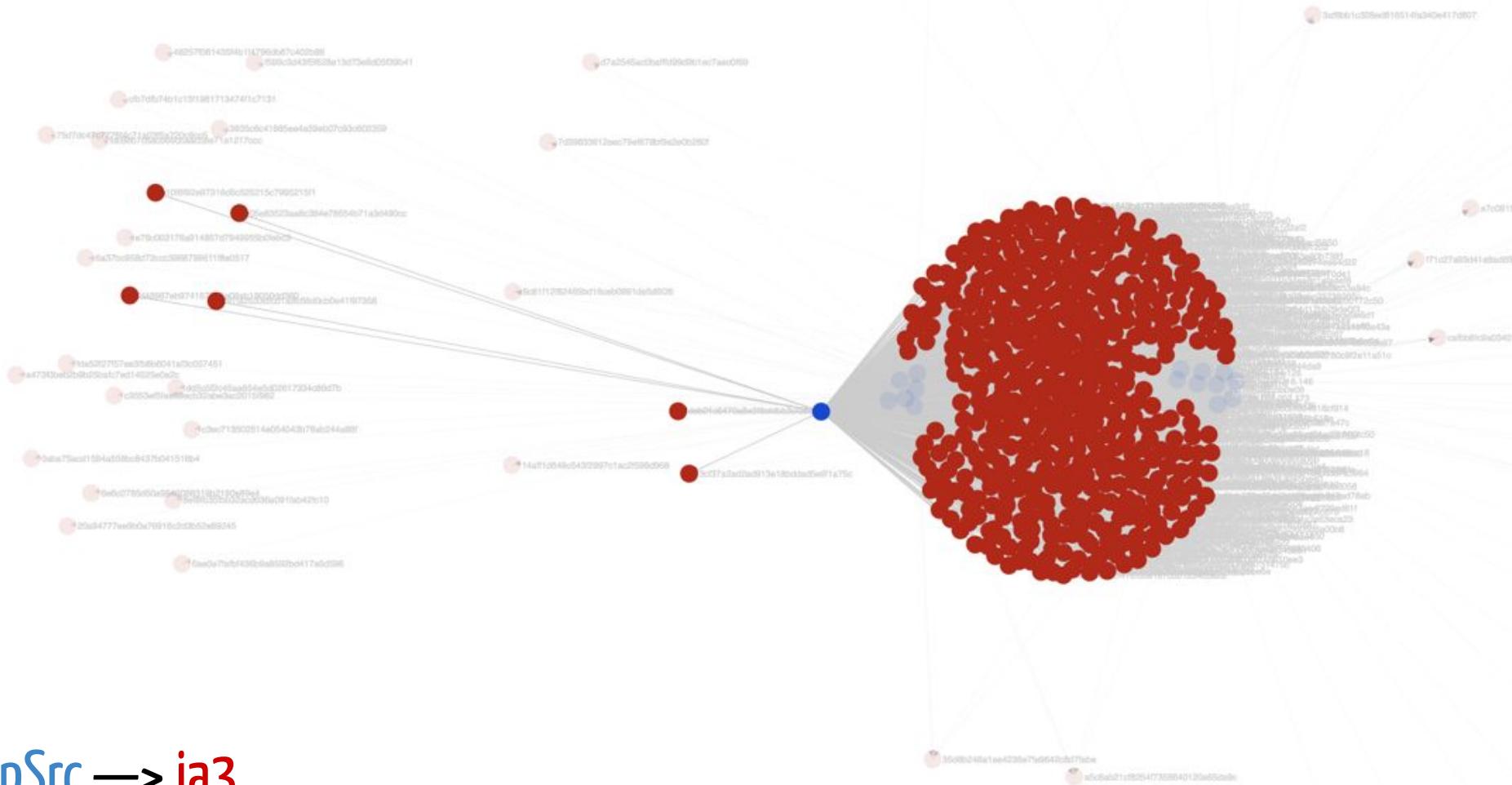
3 different actors, 3 unique patterns

They actually make themselves easier to detect by attempting to avoid fingerprinting!!

ipSrc → ja3



ipSrc → ja3



# Fingerprint Modification /evasion - I

| srcip   | dstport | ja3_hash                         | ja3_fields | ja3_str_length | request                      | tool        | org         | asn     | os          |
|---------|---------|----------------------------------|------------|----------------|------------------------------|-------------|-------------|---------|-------------|
| 184.185 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 28.185  | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 181.53  | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 216.146 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 176.220 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 207.173 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 45.103  | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 216.146 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 153.71  | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode      | AS63949 |             |
| 154.126 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode      | AS63949 |             |
| 180.112 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 172.241 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 132.213 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode      | AS63949 |             |
| .57     | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 237.43  | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              | \x15\x03\x03\x00\x02\x01\x00 | ZMAP_CLIENT | Linode, LLC | AS63949 | Linux 3.11+ |
| 253.76  | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 184.185 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 198.123 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              | \x15\x03\x03\x00\x02\x01\x00 |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 237.43  | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              | \x15\x03\x03\x00\x02\x01\x00 |             | Linode, LLC | AS63949 | Linux 3.11+ |

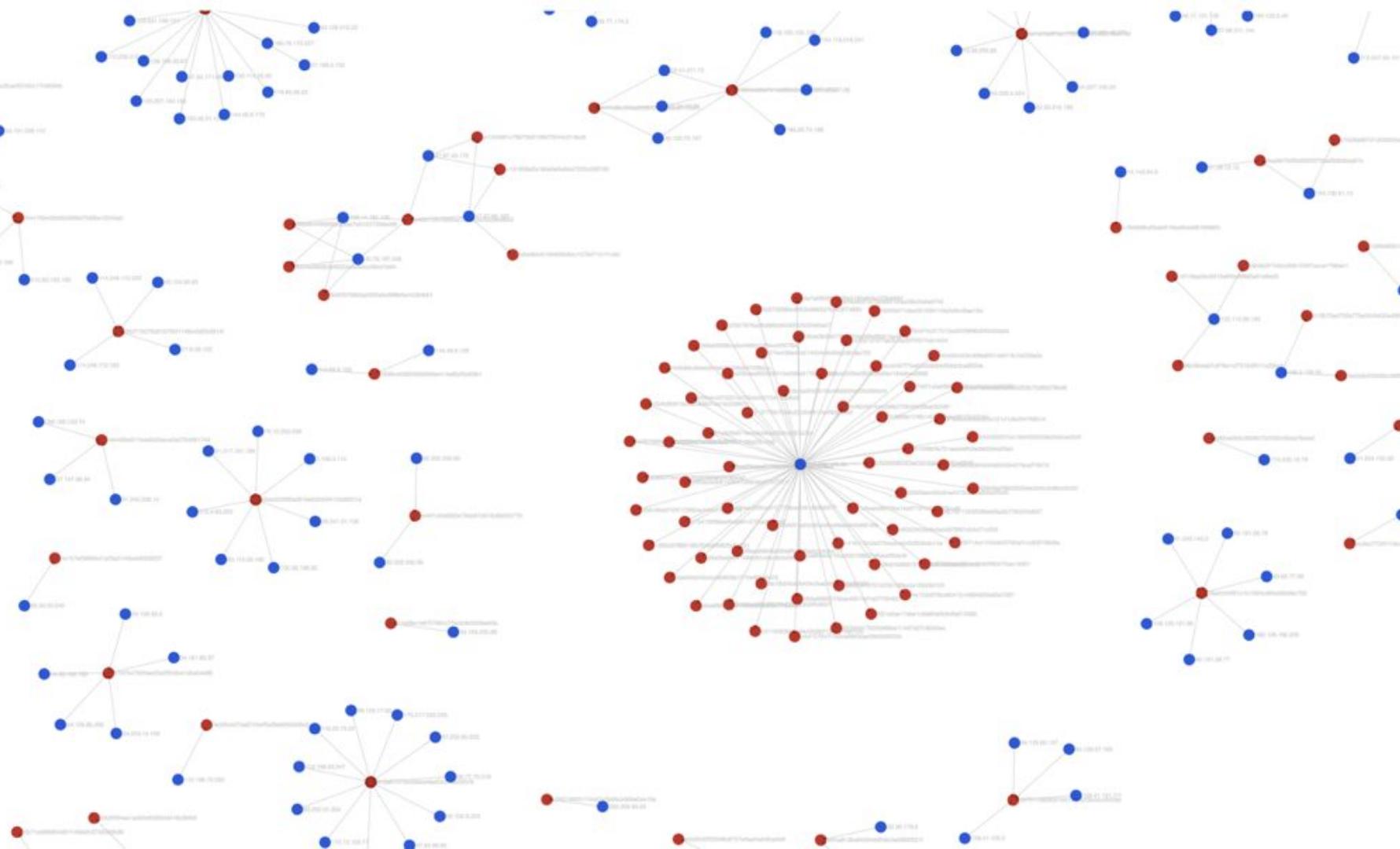
# Fingerprint Modification /evasion - I

| ja3_fields      |         | ja3_str_length                   | request     | tool                            | org         | asn         | os                  |
|-----------------|---------|----------------------------------|-------------|---------------------------------|-------------|-------------|---------------------|
| srcip           | dstport | ja3_hash                         |             |                                 |             |             |                     |
| 139.162.184.185 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11                              |             | Linode, LLC | AS63949 Linux 3.11+ |
| 178.79.128.185  | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11                              |             | Linode, LLC | AS63949 Linux 3.11+ |
| 139.162.181.53  | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11                              |             | Linode, LLC | AS63949 Linux 3.11+ |
| 151.236.216.146 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11                              |             | Linode, LLC | AS63949 Linux 3.11+ |
| 139.162.176.220 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11                              |             | Linode, LLC | AS63949 Linux 3.11+ |
| 139.162.207.173 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11                              |             | Linode, LLC | AS63949 Linux 3.11+ |
| 212.71.245.103  | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11                              |             | Linode, LLC | AS63949 Linux 3.11+ |
| 151.236.216.146 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11                              |             | Linode, LLC | AS63949 Linux 3.11+ |
| 172.104.153.71  | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11                              |             | Linode      | AS63949             |
| 172.104.154.126 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11                              |             | Linode      | AS63949             |
| 139.162.180.112 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11                              |             | Linode, LLC | AS63949 Linux 3.11+ |
| 139.162.172.241 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11                              |             | Linode, LLC | AS63949 Linux 3.11+ |
| 172.104.132.213 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11                              |             | Linode      | AS63949             |
| 185.3.94.57     | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11                              |             | Linode, LLC | AS63949 Linux 3.11+ |
| 139.162.237.43  | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11 \x15\x03\x03\x00\x02\x01\x00 | ZMAP_CLIENT | Linode, LLC | AS63949 Linux 3.11+ |
| 139.162.253.76  | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11                              |             | Linode, LLC | AS63949 Linux 3.11+ |
| 139.162.184.185 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11                              |             | Linode, LLC | AS63949 Linux 3.11+ |
| 139.162.198.123 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11 \x15\x03\x03\x00\x02\x01\x00 | ZMAP_CLIENT | Linode, LLC | AS63949 Linux 3.11+ |
| 139.162.237.43  | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,, | 11 \x15\x03\x03\x00\x02\x01\x00 | ZMAP_CLIENT | Linode, LLC | AS63949 Linux 3.11+ |
| 139.162.184.185 | 443     | d6fb7815e88dd0d8b15528b78c04b223 | 2,131200,,, | 11                              |             | Linode, LLC | AS63949 Linux 3.11+ |
| 178.79.128.185  | 443     | d6fb7815e88dd0d8b15528b78c04b223 | 2,131200,,, | 11                              |             | Linode, LLC | AS63949 Linux 3.11+ |

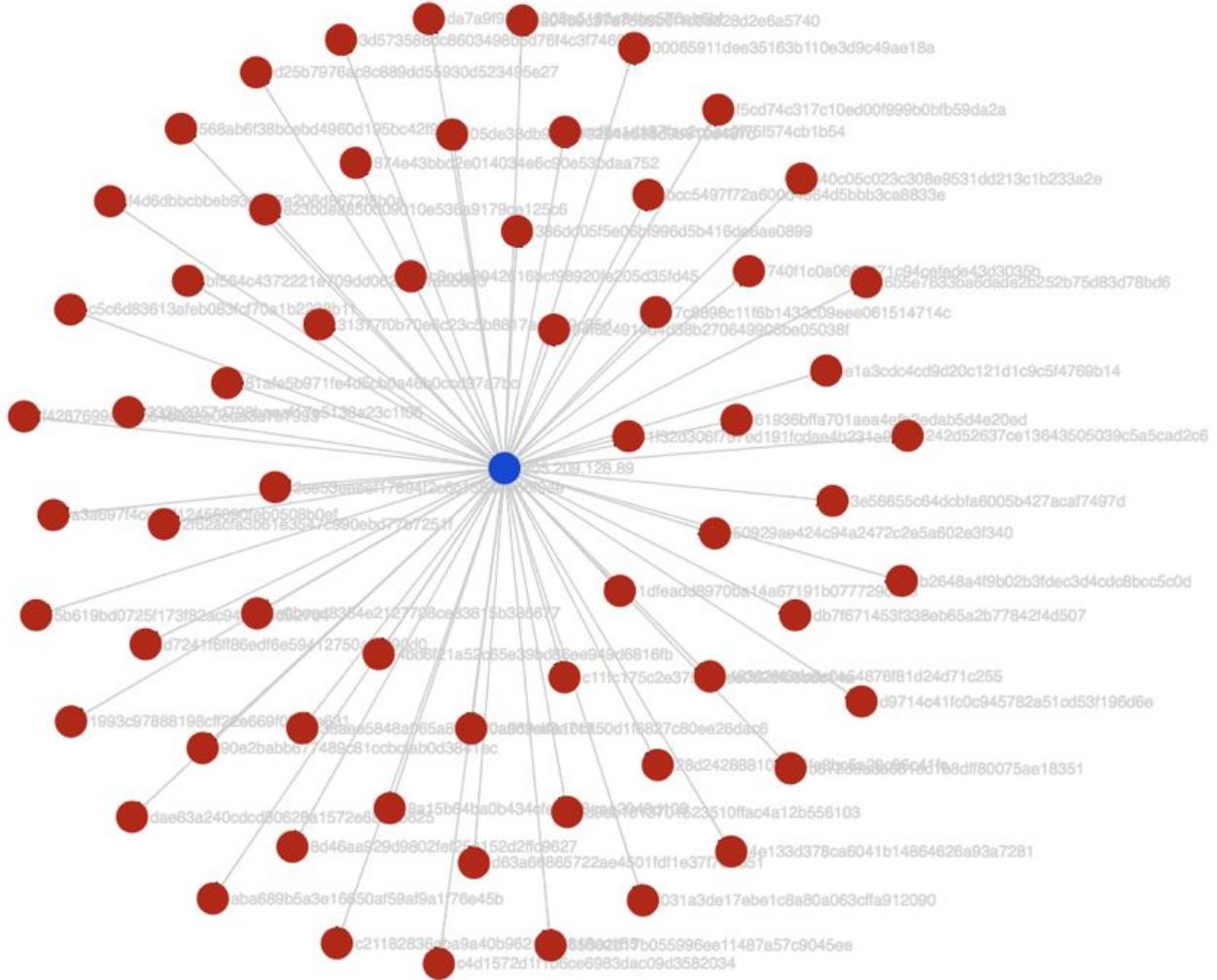
# Fingerprint Modification /evasion - I

| ja3_fields       |
|------------------|
| 768,21-255,,,    |
| 768,27-255,,,    |
| 768,49175-255,,, |
| 768,99-255,,,    |
| 768,12-255,,,    |
| 768,26-255,,,    |
| 768,9-255,,,     |
| 768,98-255,,,    |
| 768,100-255,,,   |
| 768,96-255,,,    |
| 768,97-255,,,    |
| 768,101-255,,,   |
| 768,14-255,,,    |
| 768,17-255,,,    |
| 768,20-255,,,    |
| 768,25-255,,,    |
| 768,8-255,,,     |
| 768,11-255,,,    |
| 768,23-255,,,    |
| 768,49158-255,,, |

| _time                        | srcip           | ja3_hash                          |
|------------------------------|-----------------|-----------------------------------|
| 2018-04-10T20:18:00.119+0000 | 139.162.184.185 | df092ef5e7a32dabcd42442c0037912e  |
| 2018-04-10T20:18:00.119+0000 | 139.162.184.185 | 10df32b3dcc46f4a7e481a370840519f  |
| 2018-04-10T20:18:00.119+0000 | 139.162.184.185 | faab34f1247b30b9f615903c4220076e  |
| 2018-04-10T20:18:00.119+0000 | 139.162.184.185 | 05fcf8b1aa9016b275cf79d47358771e  |
| 2018-04-10T20:18:00.123+0000 | 139.162.184.185 | e7968c3b72ecd03a7184ea034d4fec62  |
| 2018-04-10T20:18:00.123+0000 | 139.162.184.185 | f0294f0f8850c715eeadd675b7747b79  |
| 2018-04-10T20:18:00.123+0000 | 139.162.184.185 | 4283e21040c4417a3232fd4782918c16  |
| 2018-04-10T20:18:00.123+0000 | 139.162.184.185 | fee19778297abf56e541914ff74f6226  |
| 2018-04-10T20:18:00.126+0000 | 139.162.184.185 | 29bd6b9bf3f407b70f557eb2057896d8  |
| 2018-04-10T20:18:00.126+0000 | 139.162.184.185 | 5c89f4ec38319d55b7f885b7622c3a03  |
| 2018-04-10T20:18:00.126+0000 | 139.162.184.185 | 83386cbe78ad6346c0f91632747217a5  |
| 2018-04-10T20:18:00.131+0000 | 139.162.184.185 | acf5ddb3359966e4e5abc95aff84fa8   |
| 2018-04-10T20:18:00.131+0000 | 139.162.184.185 | 6846665f62c94d752775700ad8eb48ad  |
| 2018-04-10T20:18:00.131+0000 | 139.162.184.185 | 840d5724fbcd39003ecf99064d21c95e  |
| 2018-04-10T20:18:00.131+0000 | 139.162.184.185 | 965d9c52af5efc63b3fc1c78fede00f8  |
| 2018-04-10T20:18:00.131+0000 | 139.162.184.185 | 3cd877cf75cccd1b90046cb01e99c0619 |
| 2018-04-10T20:18:00.131+0000 | 139.162.184.185 | 7172b4bf900f5b30f5b24214691bfc56  |
| 2018-04-10T20:18:00.135+0000 | 139.162.184.185 | c2cc4e4ac0df30d5964b622df86c52d1  |
| 2018-04-10T20:18:00.135+0000 | 139.162.184.185 | 7063171f81740a7339d37570d3d6db84  |
| 2018-04-10T20:18:00.135+0000 | 139.162.184.185 | 618e3c499018e55d62fe52fe7a059b57  |
| 2018-04-10T20:18:00.135+0000 | 139.162.184.185 | 4ef3bbebfaefe790c233ca98d49ccb48  |



ipSrc → ja3



# Fingerprint Modification /evasion - II

# ja3\_fields

|                              |        |                                                                              |
|------------------------------|--------|------------------------------------------------------------------------------|
|                              |        | 103-51-159-107-57-136-158-69-49200-49192-49172-49199-49191-49171-61          |
| 2018-01-30T20:59:26.669+0000 | 128.89 | 29-28-65279-65278-99-101-17-114-19-115-50-64-162-116-56-106-163-49218-49238- |
| 2018-01-30T20:59:27.121+0000 | 128.89 | 103-51-159-107-57-136-158-69-49192-49172-49199-49191-49171-61                |
| 2018-01-30T20:59:27.177+0000 | 128.89 | 103-51-159-107-57-136-158-69-49172-49199-49191-49171-61                      |
| 2018-01-30T20:59:27.712+0000 | 128.89 | 103-51-159-107-57-136-158-69-49172-49199-49191-49171-61                      |
| 2018-01-30T20:59:30.305+0000 | 128.89 | 49311-49315-159-49220-49234-49221-49235-69-190-49276-136-196-49277-52394-5   |
| 2018-01-30T20:59:30.661+0000 | 128.89 | 103-51-159-107-57-136-158-69-49199-49191-49171-61                            |
| 2018-01-30T20:59:31.085+0000 | 128.89 | 103-51-107-57-136-158-69-49199-49191-49171-61                                |
| 2018-01-30T20:59:31.629+0000 | 128.89 | 103-51-57-136-158-69-49199-49191-49171-61                                    |
| 2018-01-30T20:59:32.185+0000 | 128.89 | 103-51-136-158-69-49199-49191-49171-61                                       |
| 2018-01-30T20:59:35.053+0000 | 128.89 | 103-51-158-69-49199-49191-49171-61                                           |

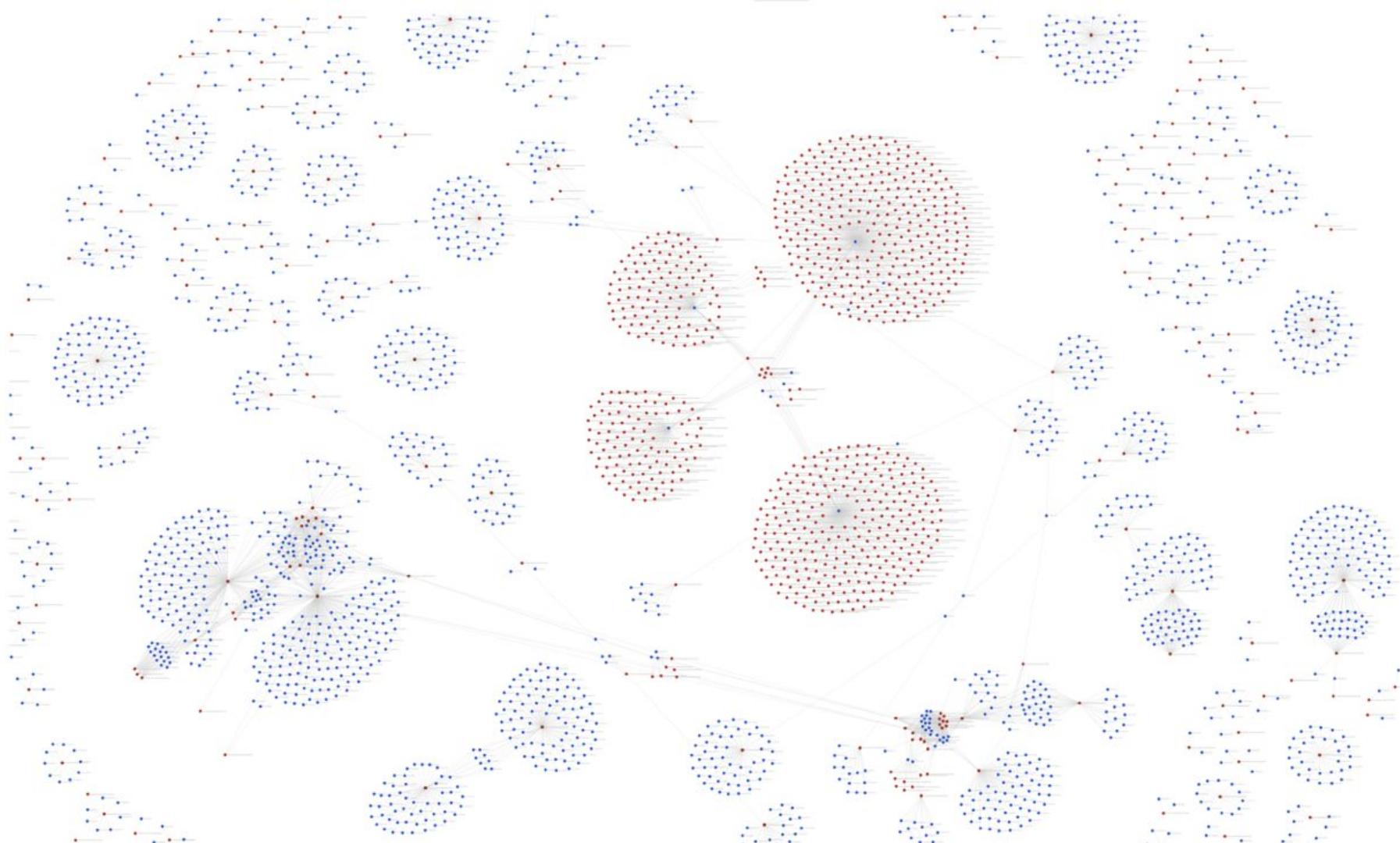
# Fingerprint Modification /evasion - II

|                              |        |                                                                              |
|------------------------------|--------|------------------------------------------------------------------------------|
|                              |        | 172-149-183-173-49256-49262-49257-49263-49304-49298-49305-49299-52398-46-184 |
| 2018-01-30T20:59:08.401+0000 | 128.89 | 185-146-124-10-125-47-60-49308-49312-156-126-53-61-49309-49313               |
| 2018-01-30T20:59:09.489+0000 | 128.89 | 185-146-124-10-125-47-60-49308-49312-156-126-53-49309-49313                  |
| 2018-01-30T20:59:10.593+0000 | 128.89 | 185-146-124-10-125-47-60-49308-49312-156-126-49309-49313                     |
| 2018-01-30T20:59:11.657+0000 | 128.89 | 185-146-124-10-125-47-60-49308-49312-126-49309-49313                         |
| 2018-01-30T20:59:12.857+0000 | 128.89 | 185-146-124-10-125-47-60-49308-49312-126-49309-49313                         |
| 2018-01-30T20:59:14.973+0000 | 128.89 | 185-146-124-10-125-47-49308-49312-126-49309-49313                            |
| 2018-01-30T20:59:16.445+0000 | 128.89 | 185-146-124-10-125-47-49308-49312-126-49309-49313                            |
| 2018-01-30T20:59:17.497+0000 | 128.89 | 185-146-124-10-125-49308-49312-126-49309-49313                               |
| 2018-01-30T20:59:18.793+0000 | 128.89 | 157-49212-49232-49213-49233-65-186-49274-132-192-49275-9-7-1-2               |
| 2018-01-30T20:59:19.849+0000 | 128.89 | 49212-49232-49213-49233-65-186-49274-132-192-49275-9-7-1-2                   |
| 2018-01-30T20:59:20.817+0000 | 128.89 | 49212-49232-49213-49233-65-186-49274-192-49275-9-7-1-2                       |
| 2018-01-30T20:59:21.613+0000 | 128.89 | 49212-49232-49213-49233-65-186-49274-192-49275-9-7-1-2                       |
| 2018-01-30T20:59:22.343+0000 | 128.89 | 49212-49232-49213-49233-186-49274-192-49275-9-7-1-2                          |
| 2018-01-30T20:59:25.547+0000 | 128.89 | 49212-49232-49213-49233-186-49274-192-49275-9-7-1-2                          |
| 2018-01-30T20:59:26.163+0000 | 128.89 | 59-4-5-150-49180-49183-49186-49179-49182-49185-49178-49181-49184             |
|                              |        | 103-51-159-107-57-136-158-69-49200-49192-49172-49199-49191-49171             |
|                              |        | 103-51                                                                       |
|                              |        | 51-103                                                                       |

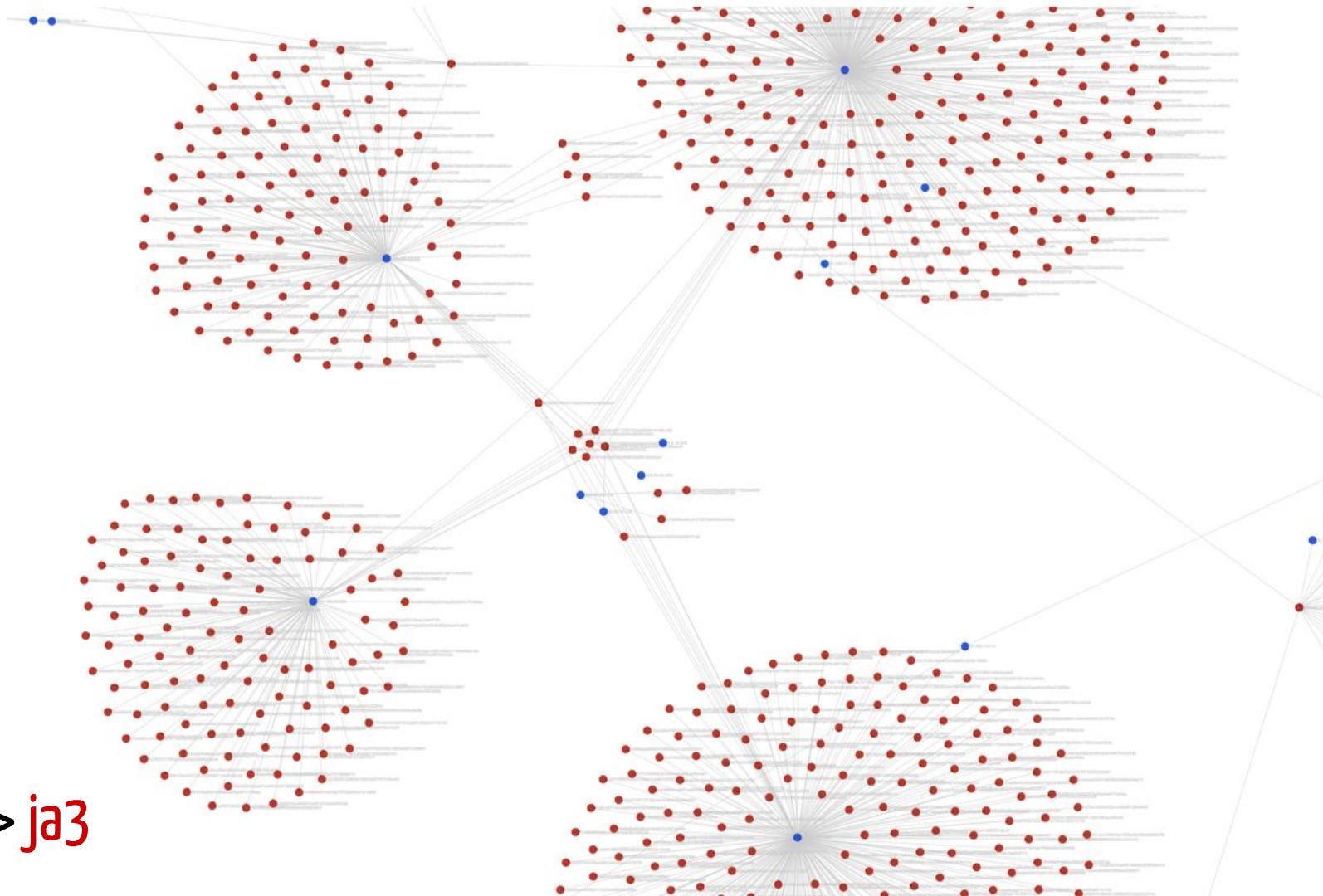
# Fingerprint Modification /evasion - II

|                                                                                           |
|-------------------------------------------------------------------------------------------|
| 49188-49325-49327-49196-49224-49244-49225-49245-49266-49286-49267-49287-52393-52244-49158 |
| 49159-49204-49205-49207-49206-49208-49264-49265-49306-49307-52396-49209-49210-49211-49203 |
| 49170-49171-49191-49199-49172-49192-49200-49228-49248-49229-49249-49270-49290-49271-49291 |
| 49170-49171-49191-49199-49172-49192-49228-49248-49229-49249-49270-49290-49271-49291       |
| 49170-49171-49191-49199-49172-49228-49248-49229-49249-49270-49290-49271-49291             |
| 49170-49171-49191-49199-49228-49248-49229-49249-49270-49290-49271-49291                   |
| 49170-49171-49191-49228-49248-49229-49249-49270-49290-49271-49291                         |
| 49170-49171-49228-49248-49229-49249-49270-49290-49271-49291                               |
| 49170-49228-49248-49229-49249-49270-49290-49271-49291                                     |

|                                                                         |
|-------------------------------------------------------------------------|
| 49303-49297-52397-45-180-181-142-20-119-22-120-51-103-49310-49314       |
| 49303-49297-52397-45-180-181-142-20-119-22-120-51-49310-49314           |
| 49303-49297-52397-45-180-181-142-20-119-22-120-49310-49314              |
| 158-121-57-107-49311-49315-159-49220-49234-49221-49235-69-190-49276-136 |
| 158-121-57-107-49311-49315-49220-49234-49221-49235-69-190-49276-136     |
| 158-121-57-49311-49315-49220-49234-49221-49235-69-190-49276-136         |
| 158-121-49311-49315-49220-49234-49221-49235-69-190-49276-136            |
| 158-121-49311-49315-49220-49234-49221-49235-69-190-49276                |
| 121-49311-49315-49220-49234-49221-49235-69-190-49276                    |
| 121-49311-49315-49220-49234-49221-49235-190-49276                       |



ipSrc → ja3



# Fingerprint Modification /evasion - III

| _time                        | srcip   | ja3                  | ja3_ciphers                                                                                                                      |
|------------------------------|---------|----------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 2018-01-12T08:09:11.794+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10<br>458944-327808-196736-65664-524416-393280-262272-131200 |
| 2018-01-12T08:09:11.842+0000 | .26.237 | e76a0619f4cf744ab2b  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                                                           |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 6b2355cd870327854d   | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                                                           |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 8d9e064b97093a2c47   | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                                                           |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                                                           |
| 2018-01-12T08:09:11.886+0000 | .26.237 | a22efd10e07be383b4c  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                                                           |
| 2018-01-12T08:09:11.934+0000 | .26.237 | 99f66d824338b066f1b  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                                                           |
| 2018-01-12T08:09:11.978+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                                                           |
| 2018-01-12T08:09:12.026+0000 | .26.237 | d5ad1a88d4c511586af  | 0-22016                                                                                                                          |
| 2018-01-12T08:09:12.072+0000 | .26.237 | a7674bf7508673e9d0e  | 148-49283-28-157-49236-49308-12-171-177-5-40-49215-49239-156-49207-69-36-11-54-82-183-27-90-49237-32                             |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 0443db5df8b9dcc91ae  | 49176-49214-177-49234-62-67-82-59-49179-50-49158-171-146-65-134-189-143-49252-49194-46-49319-49202-                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 17c9534bfc2a8edeb78  | 64-49194-75-175-76-187-49293-49296-48-39-181-38-134-49315-159-9-92-170-81-49227-126-55-137-52245-128                             |
| 2018-01-12T08:09:12.072+0000 | .26.237 | cff64173dc5b1e96141c | 49269-183-49316-49202-44-49248-49236-49163-82-49159-49229-144-49257-49185-11-54-12-186-157-67-4929                               |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 5f68c6edaa625acbb8b  | 55-191-49209-33-170-48-49203-176-49321-49169-190-49314-49182-153-49220-18-195-187-92-137-96-39-4930                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 63fa392b1105a8c4318  | 189-49205-126-167-49306-49320-49160-37-90-22-49188-134-49223-115-175-49168-63-184-88-49156-49221-49                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 5933eab69b3db48087   | 180-49306-84-49181-49254-49313-49320-49289-89-49261-184-49284-107-49269-49302-22-103-49249-49305-4                               |
| 2018-01-12T08:09:12.072+0000 | .26.237 | c6343c3579d2e0da07   | 137-96-49259-170-163-116-49199-54-49248-49200-49230-172-48-64-49269-75-145-193-70-49163-49290-53-49                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | dd6a913257a568cff93  | 65279-24-49186-57-161-49218-49162-34-165-140-49-51-49295-49233-56-150-179-98-65278-49208-49179-4919                              |
| 2018-01-12T08:09:12.073+0000 | .26.237 | 9a1b3fc416b0b64e228  | 49178-49216-49208-49279-49164-43-49265-92-49266-51-138-52245-19-49270-49307-154-160-49195-121-4919                               |
| 2018-01-12T08:09:12.118+0000 | .26.237 | 1482d0297ccdf5fdd83c | 63-30-65278-49153-147-40-49196-49171-61-29-196-79-49242-16-38-49227-49160-57-49315-52-99-49299-1-49                              |
|                              |         |                      | 49173-49317-174-49272-49190-47-42-141-49161-168-108-71-17-49240-75-175-76-187-49293-49296-64-49194-                              |

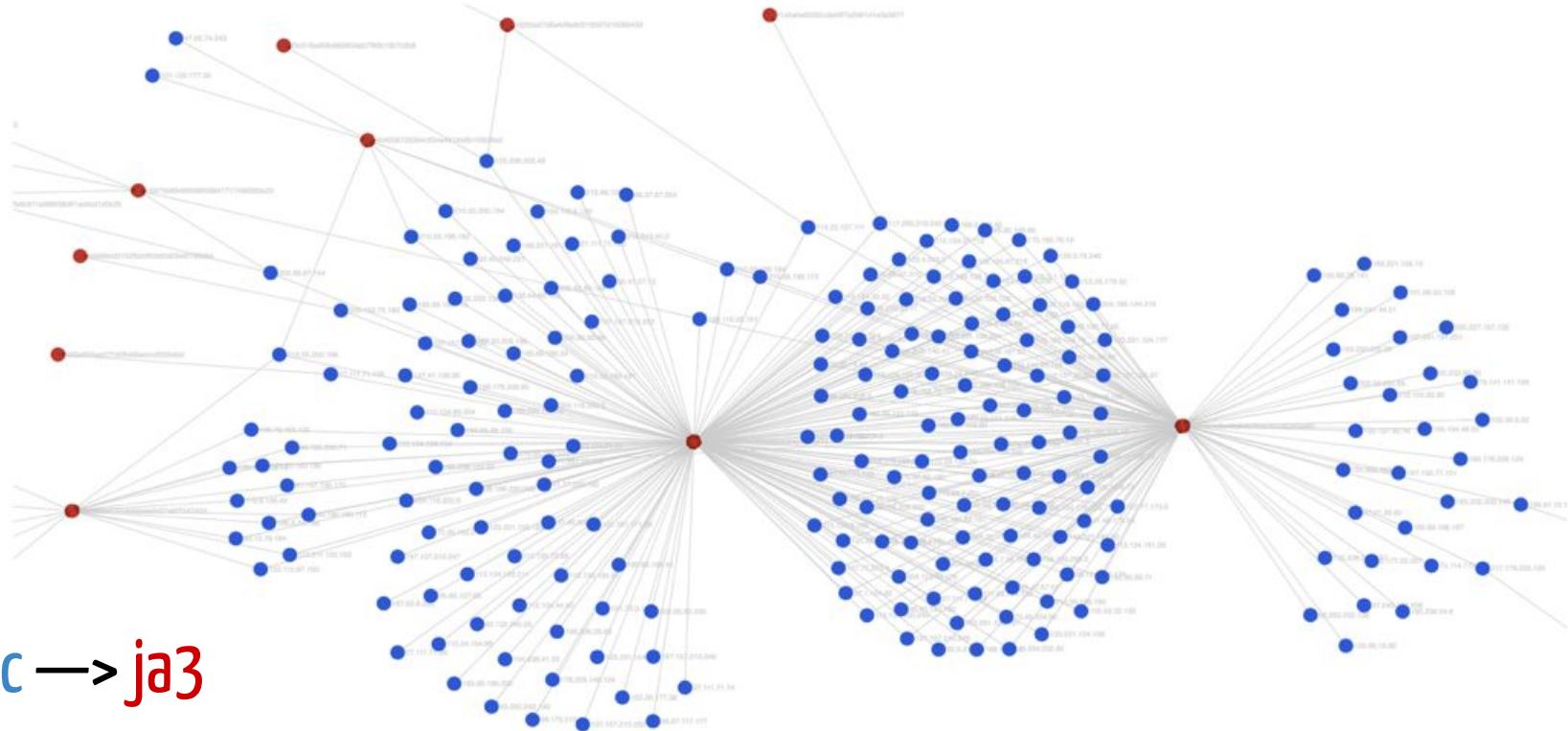
# Fingerprint Modification /evasion - III

| _time                        | srcip   | ja3                  | ja3_ciphers                                                                                           |
|------------------------------|---------|----------------------|-------------------------------------------------------------------------------------------------------|
| 2018-01-15T12:19:20.688+0000 | .26.232 | 23558e64d3f12b140t   | 5-4-2-1-22-51-57-58-24-53-10-27-47-52-49168-49158-49173-49163-49153-59-49200-49196-49192-49188-49172- |
| 2018-01-15T12:19:22.898+0000 | .26.232 | 23558e64d3f12b140t   | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.102+0000 | .26.235 | 6231f3e090902b283t   | 458944-327808-196736-65664-524416-393280-262272-131200                                                |
| 2018-02-09T09:13:30.146+0000 | .26.235 | e76a0619f4cf744ab2t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.146+0000 | .26.235 | b8aee29e75d6428de    | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.146+0000 | .26.235 | 02c79708912f096059t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.146+0000 | .26.235 | 6231f3e090902b283t   | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.186+0000 | .26.235 | 225febcb6a5c122e4c2t | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.230+0000 | .26.235 | d4cfea6a0a57b3f8edt  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.274+0000 | .26.235 | 6231f3e090902b283t   | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.318+0000 | .26.235 | 33d99dd27735072ba    | 0-22016                                                                                               |
| 2018-02-09T09:13:30.357+0000 | .26.235 | 744d459ee33c957b4t   | 49227-49201-33-183-96-19-49232-80-49175-156-3-49273-179-49199-49264-49304-49215-149-65279-182-57-53   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | e2d87fde34d1ff1f434t | 40-80-49266-157-49213-49275-81-49200-62-7-49276-124-71-126-165-49183-49185-87-24-49261-147-25-49267   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | df5779b4f188abc958t  | 79-171-16-92-49277-49168-11-187-49179-99-52243-49292-49290-49192-59-143-37-160-49284-86-24-49181-132  |
| 2018-02-09T09:13:30.357+0000 | .26.235 | a2083923440174e78t   | 72-49160-170-11-49229-197-129-49158-65278-49322-49296-46-49292-49304-114-43-49263-96-125-91-9-49166   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | aa70fd98d19f6dda13t  | 49310-49251-17-171-49234-49161-71-170-107-49231-49261-49270-49216-74-49269-173-49287-87-49188-4922    |
| 2018-02-09T09:13:30.357+0000 | .26.235 | b162bbf7959a7623at   | 49247-78-49193-52-49256-139-49164-55-135-81-49301-49205-133-49154-190-49244-49294-49170-49278-56-88   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | 9c5b4f9c58e53b744t   | 49172-10-83-14-15-158-154-49178-84-49322-49257-49261-49234-144-77-49213-49250-49291-49208-49270-180   |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 0fadcf51d6aeda5042t  | 49286-21-184-96-44-49249-49214-49274-49189-42-49306-102-49303-39-66-49263-13-49215-194-49271-49164    |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 0c8df396426c3d0539t  | 49174-49226-49268-78-162-140-22-49225-79-49250-161-38-49206-49214-66-49257-6-4-17-88-49251-180-4915   |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 542085678730261dt    | 168-49200-26-106-49323-49176-49212-49307-100-120-49182-49301-49240-49289-49201-78-49218-148-49302     |

# Profiling the tools and actors

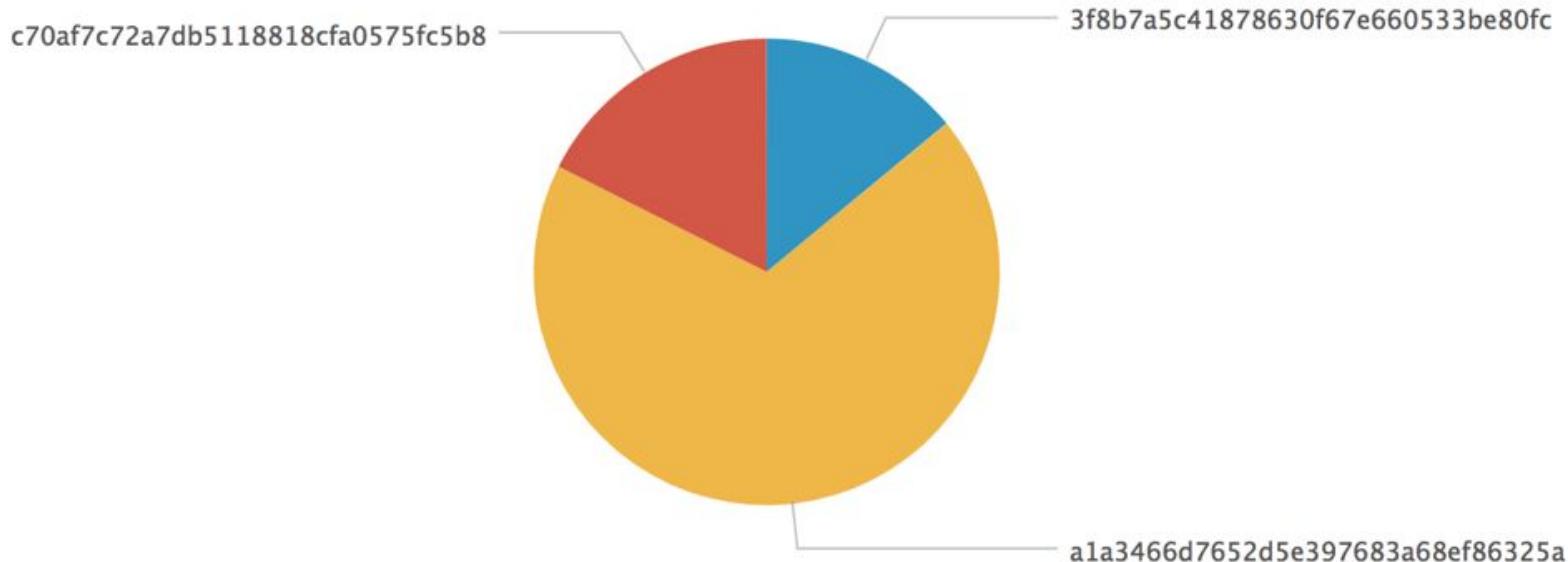
| _time                        | srcip    | dstport | ja3_hash                         | ja3_fields                  | server_name                    |
|------------------------------|----------|---------|----------------------------------|-----------------------------|--------------------------------|
| 2018-02-24T07:40:06.369+0000 | 1159.53  | 443     | eae050f0cb6163c28dd34324c1e28d74 | 771,255-49196-49195-49188-4 | <a href="#">www.bing.com</a>   |
| 2018-02-24T09:21:42.033+0000 | 1167.122 | 443     | 5001b4c2a48c94b76ca1f0199345fe60 | 771,52392-52393-49199-4920  | <a href="#">5njk.com</a>       |
| 2018-02-24T09:26:08.037+0000 | 1167.122 | 443     | 5001b4c2a48c94b76ca1f0199345fe60 | 771,52392-52393-49199-4920  | <a href="#">5njk.com</a>       |
| 2018-02-24T09:35:11.436+0000 | 1167.122 | 443     | 5001b4c2a48c94b76ca1f0199345fe60 | 771,52392-52393-49199-4920  | <a href="#">5njk.com</a>       |
| 2018-02-24T10:19:56.461+0000 | 23.69    | 443     | 5001b4c2a48c94b76ca1f0199345fe60 | 771,52392-52393-49199-4920  | <a href="#">ec22r.com</a>      |
| 2018-02-24T10:20:03.276+0000 | 23.69    | 443     | eae050f0cb6163c28dd34324c1e28d74 | 771,255-49196-49195-49188-4 | <a href="#">www.yandex.com</a> |
| 2018-02-24T10:20:04.117+0000 | 23.69    | 443     | eae050f0cb6163c28dd34324c1e28d74 | 771,255-49196-49195-49188-4 | <a href="#">www.google.com</a> |
| 2018-02-24T10:20:04.521+0000 | 23.69    | 443     | eae050f0cb6163c28dd34324c1e28d74 | 771,255-49196-49195-49188-4 | <a href="#">www.bing.com</a>   |
| 2018-02-24T10:26:20.373+0000 | 23.69    | 443     | 5001b4c2a48c94b76ca1f0199345fe60 | 771,52392-52393-49199-4920  | <a href="#">5njk.com</a>       |
| 2018-02-24T10:26:27.401+0000 | 23.69    | 443     | eae050f0cb6163c28dd34324c1e28d74 | 771,255-49196-49195-49188-4 | <a href="#">www.google.com</a> |
| 2018-02-24T10:26:27.409+0000 | 23.69    | 443     | eae050f0cb6163c28dd34324c1e28d74 | 771,255-49196-49195-49188-4 | <a href="#">www.yandex.com</a> |
| 2018-02-24T10:26:28.537+0000 | 23.69    | 443     | eae050f0cb6163c28dd34324c1e28d74 | 771,255-49196-49195-49188-4 | <a href="#">www.bing.com</a>   |
| 2018-02-24T11:53:40.309+0000 | 1167.122 | 443     | 5001b4c2a48c94b76ca1f0199345fe60 | 771,52392-52393-49199-4920  | <a href="#">mwg6aj.com</a>     |
| 2018-02-26T15:29:02.032+0000 | 248.215  | 443     | 38d1c1933f0062c7c9046659faf08872 | 771,49200-49196-49192-4918  | <a href="#">www.bing.com</a>   |
| 2018-02-26T16:34:40.229+0000 | 0.95.90  | 443     | 5001b4c2a48c94b76ca1f0199345fe60 | 771,52392-52393-49199-4920  | <a href="#">ec22r.com</a>      |
| 2018-02-26T17:07:14.321+0000 | 248.215  | 443     | 38d1c1933f0062c7c9046659faf08872 | 771,49200-49196-49192-4918  | <a href="#">5d4w7c3w.com</a>   |
| 2018-02-26T17:07:15.601+0000 | 248.215  | 443     | 38d1c1933f0062c7c9046659faf08872 | 771,49200-49196-49192-4918  | <a href="#">www.google.com</a> |
| 2018-02-26T17:07:15.940+0000 | 248.215  | 443     | 38d1c1933f0062c7c9046659faf08872 | 771,49200-49196-49192-4918  | <a href="#">www.yandex.com</a> |
| 2018-02-26T17:07:16.085+0000 | 248.215  | 443     | 38d1c1933f0062c7c9046659faf08872 | 771,49200-49196-49192-4918  | <a href="#">www.bing.com</a>   |
| 2018-02-26T17:38:10.496+0000 | 192.248  | 443     | 5001b4c2a48c94b76ca1f0199345fe60 | 771,52392-52393-49199-4920  | <a href="#">u8sj3.com</a>      |

# Profiling the tools and actors



# Discovering hidden connections /TOR Exit Nodes

- Tor=true | stats count by ja3



# Discovering hidden connections /TOR Exit Nodes

| _time                        | srcip           | ja3_hash                         |                                           | rdns                                | asn                                 | os             | tor           |
|------------------------------|-----------------|----------------------------------|-------------------------------------------|-------------------------------------|-------------------------------------|----------------|---------------|
| 2018-01-14T11:14:53.696+0000 | 163.172.84.81   | c70af7c72a7db5118818cf0575fc5b8  |                                           |                                     |                                     |                |               |
| 2018-01-14T20:38:43.548+0000 | 192.36.27.6     | c70af7c72a7db5118818cf0575fc5b8  |                                           |                                     |                                     |                |               |
| 2018-02-06T08:50:16.931+0000 | 197.231.221.211 | a1a3466d7652d5e397683a68ef86325a |                                           |                                     |                                     |                |               |
| 2018-02-06T08:50:20.755+0000 | 197.231.221.211 | a1a3466d7652d5e397683a68ef86325a |                                           |                                     |                                     |                |               |
| 2018-02-06T08:50:24.359+0000 | 93.115.86.4     | a1a3466d7652d5e397683a68ef86325a | IER_HIGH,RDP_SCANNER_LOW,HTTP_            | <a href="#">exit1.ipredator.se</a>  | AS37560                             | FreeBSD        | TRUE          |
| 2018-02-06T08:50:27.282+0000 | 93.115.86.4     | a1a3466d7652d5e397683a68ef86325a | IER_HIGH,RDP_SCANNER_LOW,HTTP_            | <a href="#">exit1.ipredator.se</a>  | AS37560                             | FreeBSD        | TRUE          |
| 2018-02-06T08:50:30.770+0000 | 93.115.86.4     | a1a3466d7652d5e397683a68ef86325a |                                           | <a href="#">lh32680.voxility.rn</a> | AS3223                              | Linux 3.1-3.10 | TRUE          |
| 2018-02-06T08:50:33.629+0000 | 93.115.86.4     | a1a3466d7652d5e397683a68ef86325a |                                           | <a href="#">lh32680.voxility.rn</a> | AS3223                              | Linux 3.1-3.10 | TRUE          |
| 2018-02-06T08:50:36.719+0000 | 185.220.101.33  | a1a3466d7652d5e397683a68ef86325a |                                           | <a href="#">lh32680.voxility.rn</a> | AS3223                              | Linux 3.1-3.10 | TRUE          |
| 2018-02-06T09:21:04.346+0000 | 204.85.191.31   | a1a3466d7652d5e397683a68ef86325a | CANNER_LOW,WEB_SCANNER_LOW                |                                     | AS200052                            | Linux 2.2-3.x  | TRUE          |
| 2018-02-06T09:21:08.866+0000 | 176.10.99.200   | a1a3466d7652d5e397683a68ef86325a | CANNER_LOW                                |                                     | <a href="#">tor01.telenet.unc</a>   | AS36850        | Linux 3.11+   |
| 2018-02-06T09:21:12.289+0000 | 176.10.99.200   | a1a3466d7652d5e397683a68ef86325a | ER_LOW,HTTP_ALT_SCANNER_LOW,WEB_SCANNER_L | <a href="#">AS51395</a>             |                                     | Linux 3.11+    | TRUE          |
| 2018-02-06T09:21:15.422+0000 | 185.38.14.171   | a1a3466d7652d5e397683a68ef86325a | ER_LOW,HTTP_ALT_SCANNER_LOW,WEB_SCANNER_L | <a href="#">AS51395</a>             |                                     | Linux 3.11+    | TRUE          |
| 2018-02-06T09:21:18.374+0000 | 185.38.14.171   | a1a3466d7652d5e397683a68ef86325a |                                           |                                     | <a href="#">tor-exit.r2.apx.pu</a>  | AS58073        | Linux 3.11+   |
| 2018-02-06T09:21:28.406+0000 | 176.126.252.11  | a1a3466d7652d5e397683a68ef86325a | CANNER_LOW                                |                                     | <a href="#">tor-exit.r2.apx.pu</a>  | AS58073        | Linux 3.11+   |
| 2018-02-06T09:21:31.755+0000 | 176.126.252.11  | a1a3466d7652d5e397683a68ef86325a | CANNER_LOW                                |                                     | <a href="#">chulak.enn.lu</a>       | AS60118        | Linux 2.2-3.x |
| 2018-02-09T01:46:43.035+0000 | 178.63.97.34    | 3f8b7a5c41878630f67e660533be80fc |                                           |                                     | <a href="#">tor-exit-01.theha</a>   | AS24940        | TRUE          |
| 2018-02-09T01:46:43.919+0000 | 178.63.97.34    | 3f8b7a5c41878630f67e660533be80fc |                                           |                                     | <a href="#">tor-exit-01.theha</a>   | AS24940        | TRUE          |
| 2018-02-09T08:39:05.874+0000 | 62.176.4.10     | 3f8b7a5c41878630f67e660533be80fc |                                           |                                     |                                     | AS34456        | Linux 3.11+   |
| 2018-02-11T11:56:19.374+0000 | 37.220.35.202   | 3f8b7a5c41878630f67e660533be80fc |                                           |                                     | <a href="#">wagyolo.10g.chn</a>     | AS58073        | Linux 3.11+   |
| 2018-02-11T11:56:19.439+0000 | 37.220.35.202   | 3f8b7a5c41878630f67e660533be80fc | FR WEB SCANNER LOW                        |                                     | <a href="#">wagyolo.10g.chn</a>     | AS58073        | Linux 3.11+   |
|                              |                 |                                  |                                           |                                     | <a href="#">tor-exit-relay-1.ai</a> | AS43847        | Linux 3.11+   |

# Observations

RDP

# Randomized Cookie String

```
{"cookie": "mstshash=axmoEEsbb", "requestedProtocols": "", "rdfp": "c1f44e11197d501693be15f474910a35"},
{"cookie": "mstshash=WpDlnTcfm", "requestedProtocols": "", "rdfp": "43ce455a5ac08b8052b1aedf97fc204b"},
{"cookie": "mstshash=RrbLtXNB1", "requestedProtocols": "", "rdfp": "0e56f411718842fab69eabf4d75f368a"},
{"cookie": "mstshash=PYYwDyELU", "requestedProtocols": "", "rdfp": "5ca4419574e2d6607846ff2dd4828417"},
{"cookie": "mstshash=qoXLlFizq", "requestedProtocols": "", "rdfp": "c1f44e11197d501693be15f474910a35"},
{"cookie": "mstshash=ixtyikeBH", "requestedProtocols": "", "rdfp": "43ce455a5ac08b8052b1aedf97fc204b"},
{"cookie": "mstshash=ZD0yuwWoI", "requestedProtocols": "", "rdfp": "0e56f411718842fab69eabf4d75f368a"},
{"cookie": "mstshash=UvsZwbgpS", "requestedProtocols": "", "rdfp": "5ca4419574e2d6607846ff2dd4828417"},
{"cookie": "mstshash=NksynyuNM", "requestedProtocols": "", "rdfp": "c1f44e11197d501693be15f474910a35"},
{"cookie": "mstshash=dZAHNUhubB", "requestedProtocols": "", "rdfp": "43ce455a5ac08b8052b1aedf97fc204b"},
{"cookie": "mstshash=KYCyNADqj", "requestedProtocols": "", "rdfp": "0e56f411718842fab69eabf4d75f368a"},
{"cookie": "mstshash=wwFTcTXqX", "requestedProtocols": "", "rdfp": "5ca4419574e2d6607846ff2dd4828417"},
{"cookie": "mstshash=LHtGaiNfu", "requestedProtocols": "", "rdfp": "c1f44e11197d501693be15f474910a35"},
{"cookie": "mstshash=eyYvKJnwQ", "requestedProtocols": "", "rdfp": "43ce455a5ac08b8052b1aedf97fc204b"},
{"cookie": "mstshash=evTHDJjuF", "requestedProtocols": "", "rdfp": "0e56f411718842fab69eabf4d75f368a"},
{"cookie": "mstshash=YzpXsNTjd", "requestedProtocols": "", "rdfp": "5ca4419574e2d6607846ff2dd4828417"},
{"cookie": "mstshash=wrFgHdesT", "requestedProtocols": "", "rdfp": "c1f44e11197d501693be15f474910a35"},
{"cookie": "mstshash=AXyfgJrRd", "requestedProtocols": "", "rdfp": "43ce455a5ac08b8052b1aedf97fc204b"},
{"cookie": "mstshash=bSlziAgmR", "requestedProtocols": "", "rdfp": "0e56f411718842fab69eabf4d75f368a"},
{"cookie": "mstshash=pFXBuTH0d", "requestedProtocols": "", "rdfp": "5ca4419574e2d6607846ff2dd4828417"}
:
```

# Different IPs, Unique RDFFP

```
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=QAMF" req_protocols=0x00000000
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=venga" req_protocols=0x00000000
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=Administrstr" req_protocols=0x00000000
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=Term1" req_protocols=0x00000000
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=Administrstr" req_protocols=0x00000000
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=Court-reg" req_protocols=0x00000000
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=pos2" req_protocols=0x00000000
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=srv" req_protocols=0x00000000
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=retail" req_protocols=0x00000000
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=POSUser" req_protocols=0x00000000
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=FPLLOGSVCU" req_protocols=0x00000000
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=alohasvc" req_protocols=0x00000000
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=qubica" req_protocols=0x00000000
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=alohaserv" req_protocols=0x00000000
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=terminal" req_protocols=0x00000000
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=Administrstr" req_protocols=0x00000000
:3389 [RDP] rdfp=6a41c49406f2d0e8175403c102ddcc06 cookie="mstshash=Administrstr" req_protocols=0x00000000
```

# JA3 of RDP Scanners

- 795bc7ce13f60d61e9ac03611dd36d90
- caadd3ed0a315543d761490b01b08e0
- c3a6cf0bf2e690ac8e1ecf6081f17a50
- d45db1e555e664b28c3a3900fd04aed9
- c369db2c355ad05c76f5660af3179b01
- 16ee84a07b55074cb2751329bf1c8811

# Observations

SSH

# Randomized SSH Client String

| client                                                                                             | hash                                             | SourceIP                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSH-2.0-Go                                                                                         | hassh(golang) = 72d744cee7c48197c1b56973e8600140 | 139.162.122.110<br>177.82.137.149<br>178.62.228.250<br>18.191.183.129<br>18.220.135.136<br>18.222.185.225<br>18.222.221.116<br>182.105.146.42<br>185.101.105.134<br>192.227.144.213<br>35.167.80.162<br>35.171.155.77<br>35.177.102.99<br>35.180.22.136<br>35.187.238.155<br>54.218.81.20<br>80.211.31.226<br>80.211.81.156<br>89.46.79.57 |
| Client string purports to be OpenSSH.<br>is always unique,<br>almost always 5char after underscore |                                                  |                                                                                                                                                                                                                                                                                                                                            |
| SSH-2.0-OpenSSH_+Zghs                                                                              | 72d744cee7c48197c1b56973e8600140                 | 119.29.145.243                                                                                                                                                                                                                                                                                                                             |
| SSH-2.0-OpenSSH_/_14mv                                                                             | 72d744cee7c48197c1b56973e8600140                 | 185.232.64.161                                                                                                                                                                                                                                                                                                                             |
| SSH-2.0-OpenSSH_03s1N                                                                              | 72d744cee7c48197c1b56973e8600140                 | 185.232.64.161                                                                                                                                                                                                                                                                                                                             |
| SSH-2.0-OpenSSH_01mQq                                                                              | 72d744cee7c48197c1b56973e8600140                 | 176.153.106.196                                                                                                                                                                                                                                                                                                                            |
| SSH-2.0-OpenSSH_2/AA9                                                                              | 72d744cee7c48197c1b56973e8600140                 | 176.153.106.196                                                                                                                                                                                                                                                                                                                            |

# Observations

gQUIC

```
{ []
 "timestamp": "2019-05-26T19:31:03.993347",
 "sourceIp": "185.200.118.46",
 "destinationIp": " [REDACTED] ",
 "sourcePort": "34870",
 "destinationPort": "443",
 "protocol": "gquic",
 "gquic": { []
 "tagNumber": "25",
 "sni": "www.google.com",
 "uaid": "Chrome/73.0.3683.103 Windows NT 10.0; Win64; x64",
 "ver": "Q043",
 "aead": "AESG",
 "smhl": "1",
 "mids": "100",
 "kexs": "C255",
 "xlct": "462969b6f5671403",
 "copt": "1330926133",
 "ccrt": "462969b6f567140367f8adc58015e3ff",
 "stk": "4bb5865849dd5dc2dccb0e62615652a31d9a9ec8e6c8669103e2c6941ee71967b46b71b4e60b26d294e6cce155a05f368f37703116bb",
 "pdmd": "X509",
 "ccs": "01e8816092921ae8",
 "scid": "ad05caad6f791c73ed603ac26b0deae0"
 }
}
```

Fake User-Agent

# Conclusion

- Network metadata and fingerprinting gives us a new perspective
- Profiling attackers and their tools
- Discovering new connections between the attackers / IPs
- Detect evasion techniques

Stay tuned for a follow-up post soon..



Thank You

@0x4d31



```
JA3
edges = df.loc[df["ja3"].notnull()].copy()
plotter = graphistry.bind(source="sourceIp", destination="ja3")
plotter.plot(edges)
```

Out[4]:

