Encrypted Things

Network Detection and Response in an Encrypted World

whoami

Patrick Perry

Technical Account Manager, Gigamon Insight

Old stuff

- 4x
- CompSci / Fuzzyvaults
- Paillier / Crypto Enthusiast
- IR consulting / GE-CIRT
- Federal Agent

Current stuff

- General Hero
- Helping customers
- Dabble in lots of things

whoami

TJ Biehle

Sr. Technical Account Manager, Gigamon Insight

Old stuff

- CompSci / parallel computing research
- IR consulting

Current stuff

- Hunt across network data
- Write code for integrations / analytics
- Write product training

Outline

1. Everything is encrypted
2. What's a security practitioner to do?
3. Metadata?
4. Use Cases!

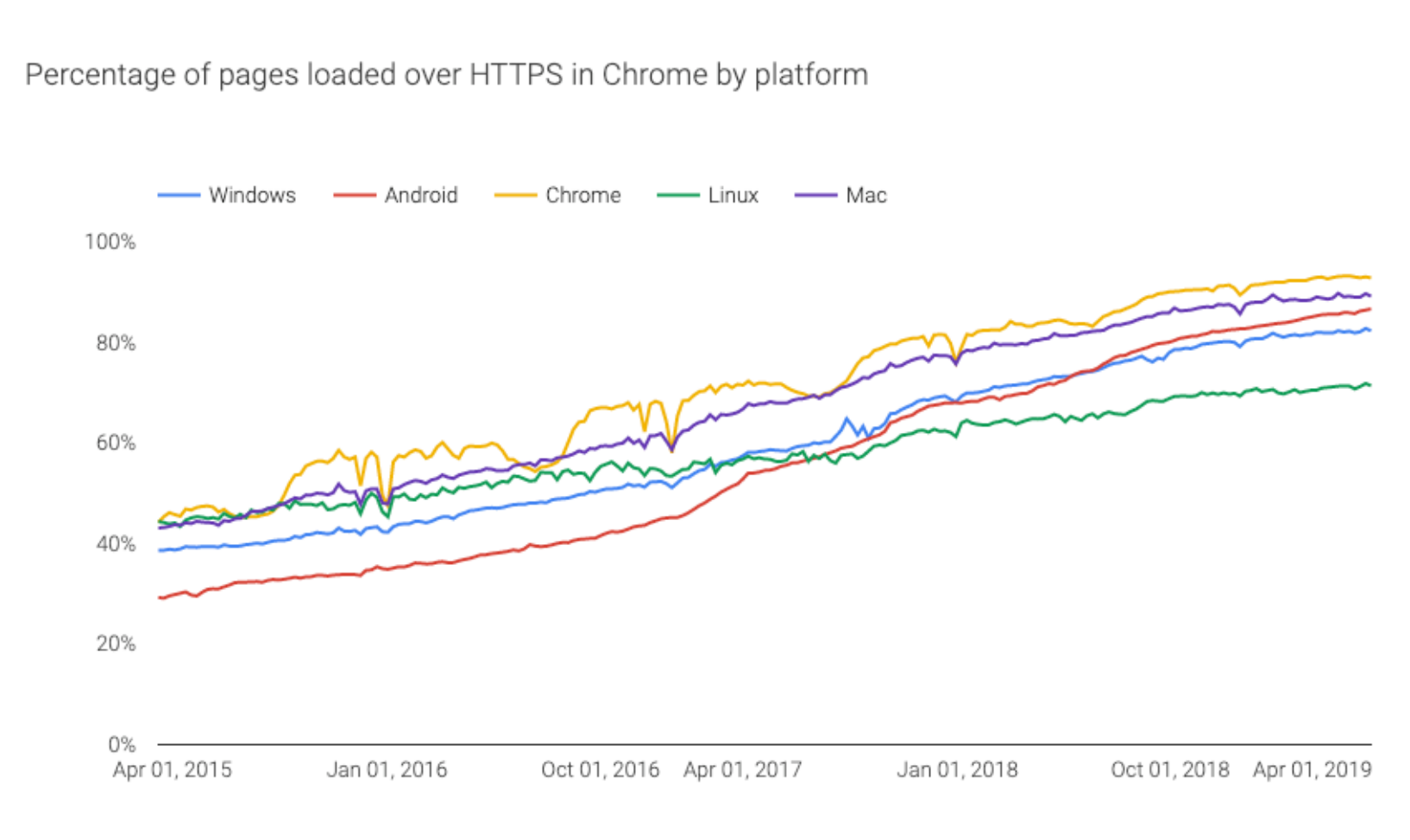
Stranger Things?

- Evil below the surface
- Bad things start to happen, most don't know when or why
- You can spot the signals once you know what to look for
- ~~We were~~ Our boss was really excited about season 3 when we wrote this talk

This talk is an update to "Network Forensics in an Encrypted World" by Will Peteroy & Justin Warner
https://www.youtube.com/watch?v=APHlvFaUEKE

(Mostly) Everything is Encrypted

Encryption Trends



- 2015 = 40-45%
- 2019 = 80-90%
- 19% growth YoY
- 2020 = 99.5%?

[1] https://transparencyreport.google.com/https/overview?hl=en

Yay privacy ...right?

Attackers can encrypt stuff too

- Payloads
- C2 channels
- Exfil / stolen goods

APT laughs at your Suri/Snort rules

Win some, lose some

WIN	
Protect from prying eyes	C
Ensure data isn’t changed	I
Verify Bob is actually Bob	Au
Prove it was actually Alice	NR

LOSE	
Can’t see malware coming in	
Can’t see data going out	
Don't lose your keys!	Av

What's a practitioner to do?

Decryption?

PROS	CONS
Everything works again	(Potential) Loss of user privacy
Encrypted and unencrypted streams = interesting analysis	Certificate management ~~can be~~ *IS* a PITA
	Things can break, badly

Metadata-based analysis?

PROS	CONS
SSL/TLS metadata isn't encrypted	Requires infrastructure to parse, store, and analyze data
Smaller = less storage $$$ / more capacity	Storage costs can still be really big with modern networks
Netflow is still a thing!*	Analysts have to know how to analyze network metadata

*Netflow is still difficult to hunt with

Decrypt or Metadata, which one?

Both!

- Metadata for HTTP + TLS
- Payload-level visibility and detection
- More data points == more analysis
- We know, we know… it’s hard

Each has its own set of challenges – there is no easy or better answer

The value of decryption / inspection is (hopefully) pretty clear

We’ll focus now on what you can do without decrypting

Analyzing TLS Metadata

TLS Metadata

These fields can be parsed from TLS traffic using ~~Bro~~ ~~Zeek~~ Bro

Field	Description
version	server's choice of SSL/TLS
cipher suite	server's choice of cipher suite
ja3	hash of Client Hello fields
ja3s	hash of Server Hello fields
SNI	host / domain client wants
server subject	server certificate attributes
server issuer	attributes of the server cert issuer
client subject	client certificate attributes
client issuer	attributes of the client cert issuer

TLS v1.3 Will Ruin Some of This

Data Source

- ~100 billion SSL/TLS sessions
- Covers 2 months of traffic
- ~50 organizations
  - All sizes
  - All industries

Version

WHAT IS IT?
String specifying SSL/TLS version used
Client suggests versions -> server chooses
NO ONE SHOULD BE USING SSLv2,3

WHAT CAN I DO WITH IT?	
Posture	✓
Detection	?
Hunting	X

WHAT DOES IT LOOK LIKE?

timestamp	type	src	dst	version
2019-07-10 07:04:25 Z	SSL	192.168.122.130:49232 (FU	124.108.101.10:443	TLSv12
2019-07-10 07:04:25 Z	SSL	192.168.122.130:49231 (FU	124.108.101.10:443	TLSv12
2019-07-10 07:04:22 Z	SSL	192.168.122.52:49336 (Jenr	23.0.202.138:443	TLSv12
2019-07-10 07:04:22 Z	SSL	192.168.122.52:49335 (Jenr	23.0.202.138:443	TLSv12

Version

- 7 unique versions observed
- 99.95% of sessions used TLS
- No TLSv1.3 yet

Version	Avg. Unique Domains	Sessions (%)
TLSv12	4,823,086	92.797
TLSv10	62,036	6.598
TLSv11	28,025	0.552
SSLv3	95	0.052
DTLSv10	15	0.0006
DTLSv12	5	0.0007
SSLv2	0	0.00003

Version

WHAT IS IT?

String specifying SSL/TLS version used

Client suggests versions -> server chooses

NO ONE SHOULD BE USING SSLv2,3

WHAT CAN I DO WITH IT?

Posture ✓

Detection ?

Hunting ✗

WHAT DOES IT LOOK LIKE?

timestamp	type	src	dst	version
2019-07-10 07:04:25 Z	SSL	192.168.122.130:49232 (FU	124.108.101.10:443	TLSv12
2019-07-10 07:04:25 Z	SSL	192.168.122.130:49231 (FU	124.108.101.10:443	TLSv12
2019-07-10 07:04:22 Z	SSL	192.168.122.52:49336 (Jenr	23.0.202.138:443	TLSv12
2019-07-10 07:04:22 Z	SSL	192.168.122.52:49335 (Jenr	23.0.202.138:443	TLSv12

Cipher Suite

WHAT IS IT?
Determines how connection is encrypted
Client suggests versions -> server chooses
Connection fails if hosts can't agree

WHAT CAN I DO WITH IT?	
Posture	✓
Detection	?
Hunting	?

WHAT DOES IT LOOK LIKE?

timestamp	type	src	dst	cipher
2019-07-10 07:04:25 Z	SSL	192.168.122.130:49232 (FU	124.108.101.10:443	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
2019-07-10 07:04:25 Z	SSL	192.168.122.130:49231 (FU	124.108.101.10:443	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
2019-07-10 07:04:22 Z	SSL	192.168.122.52:49336 (Jenr	23.0.202.138:443	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
2019-07-10 07:04:22 Z	SSL	192.168.122.52:49335 (Jenr	23.0.202.138:443	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

Cipher Suite

- 226 unique ciphers observed
- ~66% of ciphers had <10 domains
  - Tiny portion of sessions
- ~47% of ciphers had 1 domain
  - Even tinier portion of sessions

Unique Domains Over a 7-day Period

Median	Ciphers (#)	Sessions (%)
1000+	27	99.253
100+	16	0.723
10+	33	0.006
1+	48	0.003
1	102	0.000

Average	Ciphers (#)	Sessions (%)
1000+	27	99.253
100+	16	0.723
10+	34	0.013
1+	39	0.009
1	110	0.000

Cipher Suite

WHAT IS IT?

Determines how connection is encrypted

Client suggests versions -> server chooses

Connection fails if hosts can't agree

WHAT CAN I DO WITH IT?

Posture ✓

Detection ?

Hunting ?

WHAT DOES IT LOOK LIKE?

timestamp	type	src	dst	cipher
2019-07-10 07:04:25 Z	SSL	192.168.122.130:49232 (FU	124.108.101.10:443	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
2019-07-10 07:04:25 Z	SSL	192.168.122.130:49231 (FU	124.108.101.10:443	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
2019-07-10 07:04:22 Z	SSL	192.168.122.52:49336 (Jenr	23.0.202.138:443	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
2019-07-10 07:04:22 Z	SSL	192.168.122.52:49335 (Jenr	23.0.202.138:443	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

JA3 / JA3S

WHAT IS IT?

MD5 hash of a $string

$string is decimal values of the Hello bytes

JA3 == client / JA3S == server

WHAT CAN I DO WITH IT?

Posture X

Detection ✓

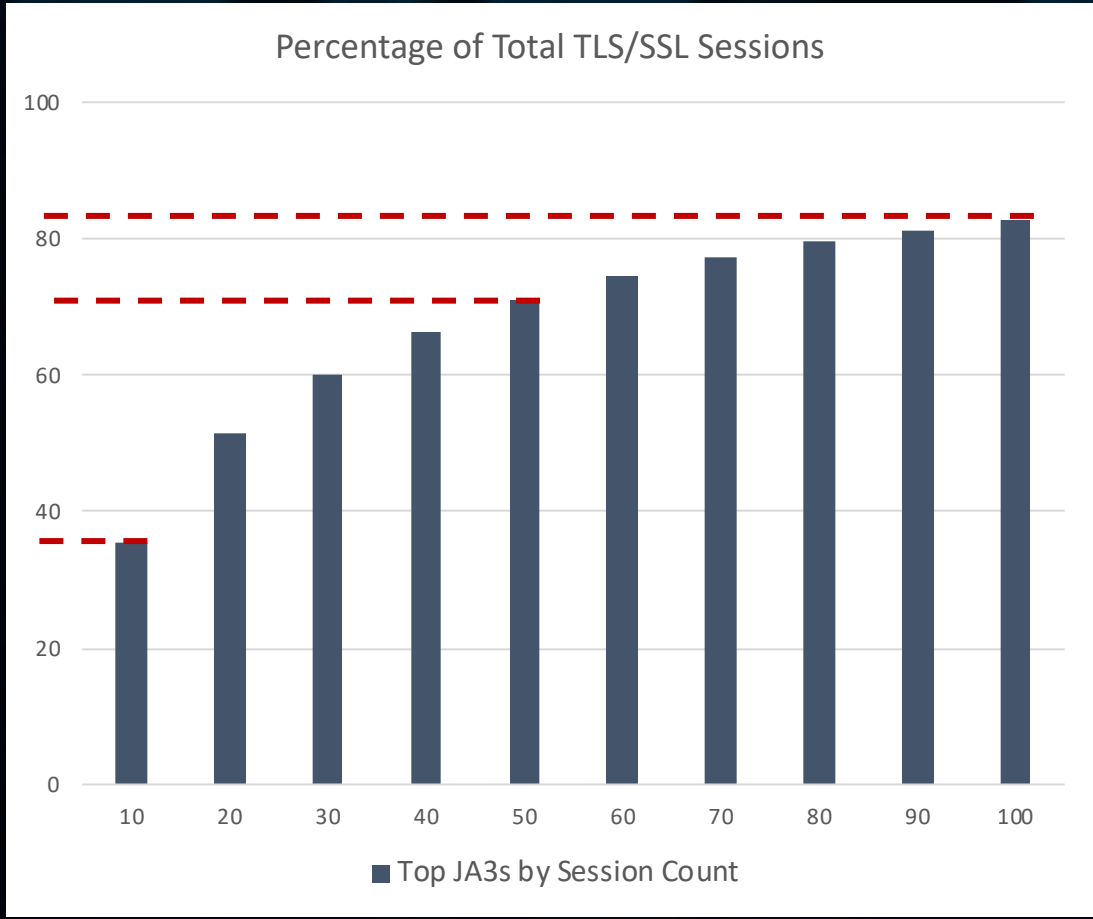
Hunting ✓

WHAT DOES IT LOOK LIKE?

timestamp	type	src	dst	ja3	server_name_indication
2019-07-10 07:01:04 Z	SSL	192.168.122.52:49158 (Jenr	119.160.243.163:443	4d7a28d6f2263ed61de88ca66eb011e3	search.yahoo.com
2019-07-10 07:01:04 Z	SSL	192.168.122.52:49159 (Jenr	119.160.243.163:443	4d7a28d6f2263ed61de88ca66eb011e3	search.yahoo.com
2019-07-09 08:19:30 Z	SSL	10.1.70.200:51613 (Develope	74.119.119.66:443	10ee8d30a5d01c042afd7b2b205facc4	gum.criteo.com
2019-07-09 08:19:30 Z	SSL	10.1.70.200:51610 (Develope	74.119.119.66:443	10ee8d30a5d01c042afd7b2b205facc4	gum.criteo.com
2019-07-09 08:19:29 Z	SSL	10.1.70.200:51609 (Develope	74.119.119.66:443	10ee8d30a5d01c042afd7b2b205facc4	gum.criteo.com

JA3

- 215,803 unique ja3 observed
- Small number of ja3 observed in large portion of sessions
  - Top 10 = 36%
  - Top 50 = 71%
  - Top 100 = 83%
- Modest amount of intel work yields a significant enrichment



JA3

- Quick and dirty intel process
  - ja3er.com
  - useragentstring.com
- Yields results for 51 of the top 100
- Not-too-much python™ yields helpful context
  - “Weird” ja3
  - Powershell / LOLbin talking out

User Agent String.Com

Home | List of User Agent Strings | Links | API |

User Agent String explained :

```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:69.0) Gecko/20100101 Firefox/69.0
```

Copy/paste any user agent string in this field and click 'Analyze' Analyze

Firefox 69.0

Mozilla	MozillaProductSlice. Claims to be a Mozilla based user agent, which is only true for Gecko browsers like Firefox and Netscape. For all other user agents it means 'Mozilla-compatible'. In modern browsers, this is only used for historical reasons. It has no real meaning anymore
5.0	Mozilla version
Macintosh	Platform
Intel Mac OS X 10.14	Operating System: OS X Version 10.14 : running on a Intel CPU
rv:69.0	CVS Branch Tag The version of Gecko being used in the browser
Gecko	Gecko engine inside
20100101	Build Date: the date the browser was built
Firefox	Name : Firefox

JA3S

- 424 unique ja3s observed
- ~69% of ja3s had <10 domains
  - Tiny portion of sessions
- ~40% of ja3s had 1 domain
  - Even tinier portion of sessions

Unique Domains Over a 7-day Period

Median	JA3S (#)	Sessions (%)
1000+	47	99.142
100+	37	0.779
10+	46	0.038
1+	145	0.038
1	149	0.003

Average	JA3S (#)	Sessions (%)
1000+	47	99.142
100+	37	0.779
10+	46	0.038
1+	119	0.038
1	175	0.003

JA3 / JA3S

WHAT IS IT?

MD5 hash of a $string

$string is decimal values of the Hello bytes

JA3 == client / JA3S == server

WHAT CAN I DO WITH IT?

Posture X

Detection ✓

Hunting ✓

WHAT DOES IT LOOK LIKE?

timestamp	type	src	dst	ja3	server_name_indication
2019-07-10 07:01:04 Z	SSL	192.168.122.52:49158 (Jenr	119.160.243.163:443	4d7a28d6f2263ed61de88ca66eb011e3	search.yahoo.com
2019-07-10 07:01:04 Z	SSL	192.168.122.52:49159 (Jenr	119.160.243.163:443	4d7a28d6f2263ed61de88ca66eb011e3	search.yahoo.com
2019-07-09 08:19:30 Z	SSL	10.1.70.200:51613 (Develope	74.119.119.66:443	10ee8d30a5d01c042afd7b2b205facc4	gum.criteo.com
2019-07-09 08:19:30 Z	SSL	10.1.70.200:51610 (Develope	74.119.119.66:443	10ee8d30a5d01c042afd7b2b205facc4	gum.criteo.com
2019-07-09 08:19:29 Z	SSL	10.1.70.200:51609 (Develope	74.119.119.66:443	10ee8d30a5d01c042afd7b2b205facc4	gum.criteo.com

Server Name Indicati n (SNI)

WHAT IS IT?

How a client specifies which ho

It's a domain – yo
would norma

WITH IT?

ng ✓

LIKE?

timestamp			dst	server_name_indication
2019-07-10 07:04:22 Z	S	2:49335 (Jenn	23.0.202.138:443	static.tacdn.com
2019-07-10 07:04:22 Z	SSL	68.122.52:49334 (Jenn	104.97.224.191:443	www.tripadvisor.co.nz
2019-07-10 07:04:11 Z	SSL	192.168.122.52:49309 (Jenn	103.2.116.79:443	www.google.com
2019-07-10 07:04:11 Z	SSL	192.168.122.52:49308 (Jenn	103.2.116.79:443	www.google.com

SNI + TLS 1.3

- SNI was always an optional extension – common, but optional
- TLS 1.3 gives the option to encrypt the SNI
  - Via DNS (it's always DNS)

Why encrypt the SNI?

- Privacy
- ISPs, coffee shop sniffers, etc. shouldn't get to snoop

Certificate attributes

WHAT IS IT?

Contents of the Subject and Issuer fields

Server cert is usually required

Client cert is usually not required

WHAT CAN I DO WITH IT?

Posture ✓

Detection ✓

Hunting ✓

WHAT DOES IT LOOK LIKE?

timestamp	type	src	dst	subject	issuer
2019-07-10 07:02:02 Z	SSL	192.168.122.130:49191 (FU	203.84.197.9:443	CN=www.yahoo.com,O=Yahoo Inc.,L=Sunnyvale,ST=California,C=US	CN=Symantec Class 3 Secure Server CA - G4
2019-07-10 07:02:02 Z	SSL	192.168.122.130:49189 (FU	68.232.45.200:443	CN=*.vo.msecnd.net	CN=Microsoft IT SSL SHA2,OU=Microsoft IT
2019-07-10 07:02:02 Z	SSL	192.168.122.130:49190 (FU	68.232.45.200:443	CN=*.vo.msecnd.net	CN=Microsoft IT SSL SHA2,OU=Microsoft IT
2019-07-10 07:02:00 Z	SSL	192.168.122.130:49188 (FU	119.160.254.215:443	CN=*.yimg.com,O=Yahoo Inc.,L=Sunnyvale,ST=California,C=US	CN=Symantec Class 3 Secure Server CA - G4
2019-07-10 07:01:59 Z	SSL	192.168.122.130:49187 (FU	119.160.254.215:443	CN=*.yimg.com,O=Yahoo Inc.,L=Sunnyvale,ST=California,C=US	CN=Symantec Class 3 Secure Server CA - G4
2019-07-10 07:01:59 Z	SSL	192.168.122.130:49186 (FU	119.160.254.215:443	CN=*.yimg.com,O=Yahoo Inc.,L=Sunnyvale,ST=California,C=US	CN=Symantec Class 3 Secure Server CA - G4

Certificate attributes + TLS 1.3

- Why encrypt the certificates?
  - Same reasons as SNI, namely privacy
  - Not encrypting certs would undermine encrypting the SNI

TLS Metadata and You

Use Cases!

Let's divide analysis work into three categories

- Detection
- Hunting
- Posture

The next few slides will explore use cases for each

Detection

Best applies to tracking known compromises

- Careful with lists of “OSINT”

Is the value unique / uncommon

- If yes, detect!
- If no, false-positives galore!

Upside: JA3/cipher suites focus on <u>how</u> instead of <u>who</u>

Detection

timestamp	type	src	dst
2019-07-08 07:01:37 Z	SSL	10.10.10.209:49250 (Batiste-	86.61.160.5 :4 7

server_name_indication	subject	issuer
	CN=sd-97597.dedibox.fr	CN=sd-97597.dedibox.fr

ja3	ja3s	cipher
6734f37431670b3ab...	5e4e5596180ebd0a...	TLS_ECDHE_RSA_WITH_AES...

Detection – GREENCAT

- Known useragents
- Specific uri patterns
- Requires decrypted HTTP proxy traffic.

Detection – MACKTRUCK / ROADHOUSE

- Specific certsubject
- Specific issuersubject
- Specific SHA1
- Specific serial
- Leveraging metadata

Detection – Powershell

- Powershell SSL traffic
- Issuer = Let’s Encrypt
- JA3 Hash

Detection - Reductor

- https://securelist.com/compfun-successor-reductor/93633/
- Watermarking TLS handshake
- Subverted PRNG
- SHA1 fingerprint

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            fa:9b:b7:53:21:86:97:bd:ed:1a:8c:85:59:fb:f6:94
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C = EN, CN = GeoTrust Rsa CA, O = GeoTrust Rsa CA
        Validity
            Not Before: Oct 23 22:56:10 2011 GMT
            Not After : Nov 17 22:56:10 2031 GMT
        Subject: C = EN, CN = GeoTrust Rsa CA, O = GeoTrust Rsa CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:d1:02:fa:c5:94:71:f2:45:4e:80:b9:ee:08:61:
                    ed:6b:c6:2c:3a:df:c7:99:48:a7:4c:ab:64:31:22:
```

Hunting

The purpose of hunting is to find things you didn’t know about

Typically looking for attackers / compromises

- Who are we interacting with?
- How are we interacting with them?

May (probably will) uncover some security posture / hygiene issues

Hunting

	WHO ARE WE INTERACTING WITH?	HOW ARE WE INTERACTING
Fields	SNI Certificate Attributes	Cipher Suite JA3 / JA3S

Q's	• How many hosts are talking to this entity?
	• When was the first time we saw this entity?
	• When was this entity registered?
	• Who owns the entity?
	• Is there anything odd about this entity?
	  • Uncommon TLD
	  • Random-looking
	  • Name/typo squatting
		• How many hosts are showing this entity?
		• What software is related to this entity?

Hunting

```
ja3 <> null group by ja3, min(timestamp)
```

ja3	min(timestamp)
0512f612d3d51fbafda36ffb6310482a	2019-07-09 18:52:08
043a5d2d936910298e36e34acd8da818	2019-07-09 18:52:06
de598a1957d57cbc201ca2655b808b27	2019-06-24 22:53:06
bcac05401eaa3573485983e846dd7217	2019-06-24 22:52:47
7189a3919e2935485d9cc4012eca1883	2019-06-14 19:16:22
4056657a50a8a4e5cfac40ba48becfa2	2019-06-14 16:16:40
32926ca3e59f0413d0b98725454594f5	2019-06-13 22:21:19

Hunting

Here's how we parse the user agent:

```
Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0 (count: 13, last seen: 2019-06-12 12:27:54)
```

Firefox 60 on Linux

Here's detailed information about it:

Simplified readout

Clear, human readable descriptions of the software & platform

Simple Software String
Firefox 60 on Linux

Simple Sub-description

Simple Operating Platform

Software

Information about the web software

Software
Firefox 60

Software Name
Firefox

Software Name Code

Operating System

Information about the Operating System

Operating System
Linux

Operating System Name
Linux

Operating System Name Code

https://developers.whatismybrowser.com/useragents/parse/

Hunting

JA3 SSL Fingerprint

Sorry the hash

0512f612d3d51fbafda36ffb6310482a

was not found in the database. If you have further info to this hash please comment below.

Hunting

```
ja3 = '0512f612d3d51fbafda36ffb6310482a' group by dst.asn.asn_org
```

dst.asn.asn_org	count
Google LLC	1,020
Rochester Institute of Technology	552
Akamai Technologies, Inc.	320
Amazon.com, Inc.	232
Integral Ad Science, Inc.	156
Cloudflare, Inc.	140
Fastly	106
Highwinds Network Group, Inc.	104
Facebook, Inc.	86
AppNexus, Inc	38

Google / Amazon +

Advertising +

CDNs +

Social Media +

...workstation web browser?

...recently updated web browser?

Hunting Recap

Quick look at new JA3 hashes

- Only covered 30 days of data
- We could have seen those hashes 40 days ago

Better way: Intel team tracks all observed JA3 hashes and alerts on hashes never seen before

- Software updates = new hashes (maybe)
- Prevalence is important

Same could be done for certificates / domains

Posture

No one should be using any version of SSL

- Do you have internal systems that support it?
- Do you have externally-facing systems that support it?
- Do any of your vendors support it?

Could also look at deprecated cipher suites

Posture

```
ssl:version IN ('SSLv2', 'SSLv3') AND dst.internal = false group by server_name, version
```

server_name	version	count
cm2.[redacted].com	SSLv3	21
www.ssllabs.com	SSLv3	2

Wrap Up

Takeaways

- Encryption is here to stay
- Decryption + metadata is ideal, both have pros/cons
- There is plenty of analysis to be done on TLS metadata
  - TLS v1.3 will hinder analysis on who
  - But, it won’t hinder analysis on how
- We need to put in some work on JA3 intel

Questions?