When Intrusions Don’t Align: A New Water Watering Hole and Oldsmar

dragos.com/blog/investigating-the-watering-hole-linked-to-the-oldsmar-water-treatment-facility-breach/

May 18, 2021

Blog Post

By Kent Backman

05.18.21

Members of the cybersecurity community at large know that learning opportunities present themselves every day. The purpose behind this investigative anecdote on the “water watering hole” is educational and highlights how sometimes two intrusions just don’t line up together no matter how much coincidence there is. We hope you will agree after reading this that intelligence and intrusion analysis are not always what they seem.

Our story begins in Oldsmar, Florida, on Monday, 08 February 2021, when the Pinellas County Sheriff held a press conference. The sheriff, Oldsmar mayor, and city manager described a water poisoning attempt at the city’s water treatment plant the previous Friday. This unprecedented event made both a stir in the media and among Dragos’s team of adversary hunters.

A Water Watering Holels Discovered

During our investigation into the infamous water poisoning attempt against the citizens of Oldsmar, Dragos discovered a Florida water utility contractor hosting malicious code on their website (i.e., a watering hole). This malicious code seemingly targeted water utilities, particularly in Florida, and more importantly, was visited by a browser from the city of Oldsmar on the same day of the poisoning event.

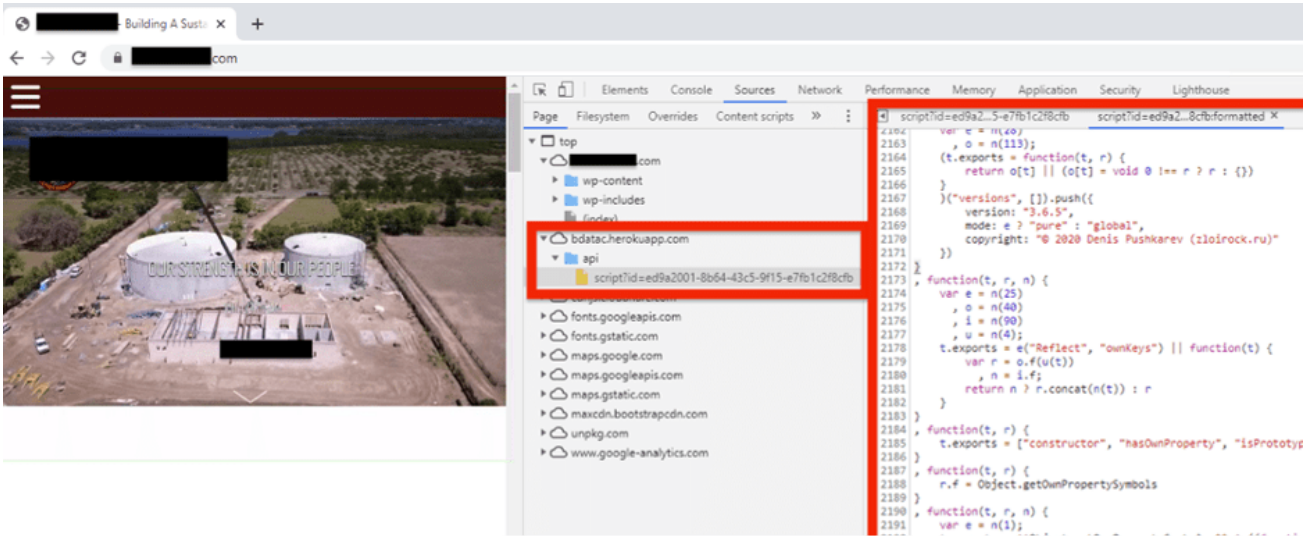

Figure 1: Website compromised with a unique browser enumeration and fingerprinting script

The adversary inserted the malicious code into the footer file (Figure 2) of the WordPress-based site associated with a Florida water infrastructure construction company. The adversary possibly exploited one of the multiple vulnerable WordPress plugins that Dragos determined were in use on the site at the time of compromise.

Figure 2: Location of the subverted code in the footer of the once compromised WordPress site xxxxxxxxxxxxx[.]com

A Snapshot of the Malicious Data Gathering Campaign

This malicious data gathering campaign affected computer systems that browsed the compromised, but otherwise legitimate, website during a 58-day window beginning 20 December 2020. Dragos assisted with malicious code identification and initial remediation of the compromised website on 16 February 2021. Those who interacted with the malicious code included computers from municipal water utility customers, state and local government agencies, various water industry-related private companies, and normal internet bot and website crawler traffic. Over 1000 end-user computers were profiled by the malicious code during that time, mostly from within the United States and the State of Florida, as shown in Figure 3.

Figure 3: Geolocation of US fingerprinted client computers

Using telemetry from Team Cymru Pure Signal Recon, Dragos determined that a user on a computer system on a network belonging to the City of Oldsmar browsed the compromised site at exactly 14:49 Coordinated Universal Time (UTC), or 9:49 am on 05 February 2021. This is the same network where an unknown actor reportedly compromised a water treatment control plant computer on the morning of 05 February and attempted to poison the water supply using the computer system's Human Machine Interface (HMI).

Based on these initial facts Dragos released an Advisory Alert on 17 February 2021 to customers informing them of the watering hole potentially targeting water utilities along with defensive guidance and indicators. The purpose of an Advisory Alert is to ensure customers receive and can act on timely intelligence when the entire story is not yet known. We also shared our insights with our partners at the Department of Homeland Security (DHS) so they could perform victim notifications if they deemed it important.

After the Advisory Alert Dragos went to work uncovering and exposing the entire threat.

Deciphering the Malicious Fingerprinting Script

Dragos reverse-engineered the fingerprinting script and determined it used code from four different code projects: core-js, UAParser, regeneratorRuntime, and a data collection script only observed elsewhere on two websites (website 1, website 2) associated with a domain registration, hosting, and web development company.

The fingerprinting script gathered over 100 elements of detailed information about the visitors including the following:

- Operating system and CPU
- Browser, including available languages
- Touch points, input methods, presence of camera, accelerometer, microphone
- Video card display adapter details, and
- Time zone, geolocation, video codecs, screen dimensions, browser plugins

The script also directed the visiting browser to two separate browser cipher fingerprinting sites to collect cipher fingerprint hashes: TLS fingerprint, JA SSL Fingerprint. Various network defense regimes typically compute browser cipher fingerprinting such as JA3 (done by ja3er[.]com, for example) to detect connections from malware-infected hosts and discern hostile connections from legitimate browser client traffic. Once all this data was collected in the browser memory, the JavaScript code sent the data via Hypertext Transfer Protocol (HTTP) POSTs to a database on the same Heroku app site that hosted the script, bdatac.herokuapp[.]com. This Heroku app was taken down after notification from Dragos.

Dragos found exactly one other internet site that hosted this complex code and served it to visiting internet browsers, DarkTeam Store. DarkTeam Store claims to be a dark market that supplies thousands of customers with gift cards and accounts (Figure 4).

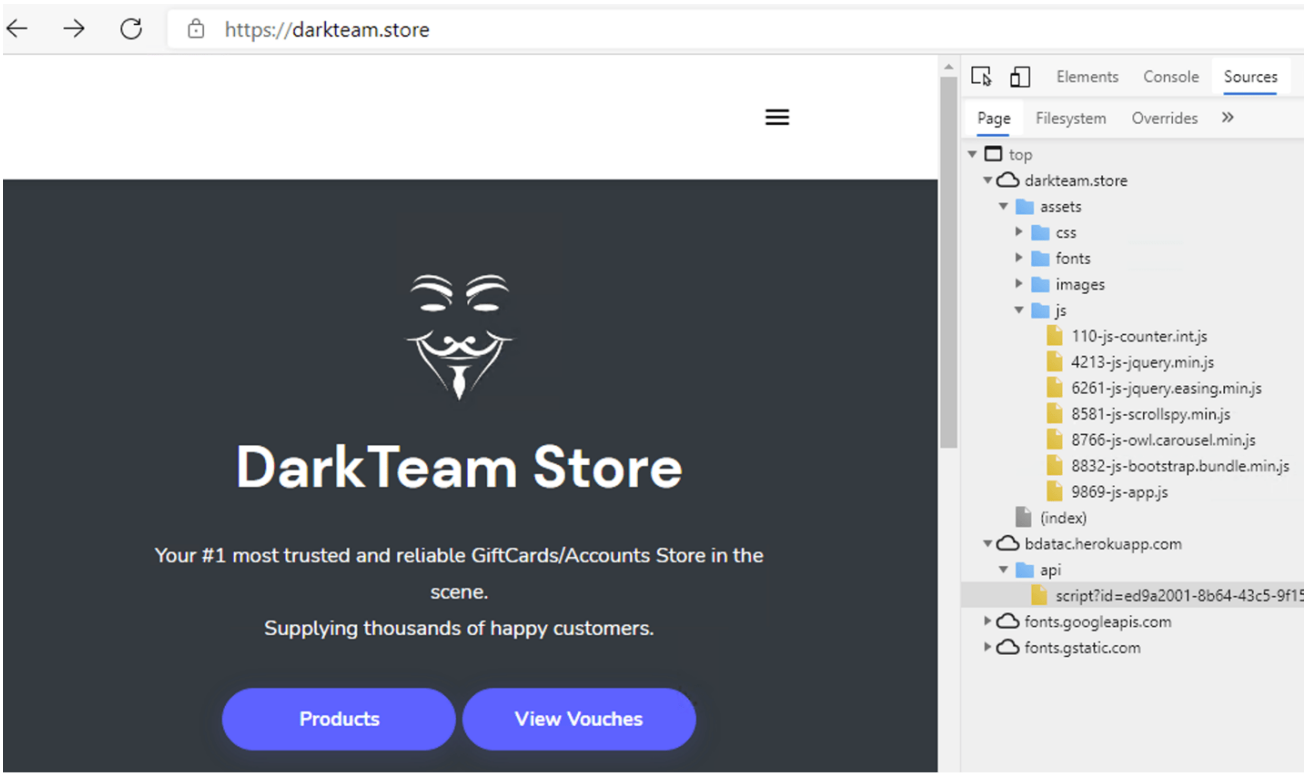

Figure 4: Browser enumeration and fingerprinting script on purported dark market site darkteam.store

Additional analysis of data obtained by Dragos revealed that at least a portion of this site may not actually be a dark market, but rather a check-in place for systems infected with a recent variant of botnet malware known as Tofsee. Dragos found evidence showing that the DarkTeam store and the water infrastructure construction company website were subverted by the same actor on the same day (20 December 2020). Dragos observed 12,735 IP addresses representing likely Tofsee-infected systems worldwide employing 271 unique user agents. These clients connected to a non-public (i.e., requiring authentication) page (httpx://darkteam[.]store/dogs/Home-2.html) of the DarkTeam site and presented a browser user agent string with a peculiar “Tesseract/1.0” artifact (Figure 5).

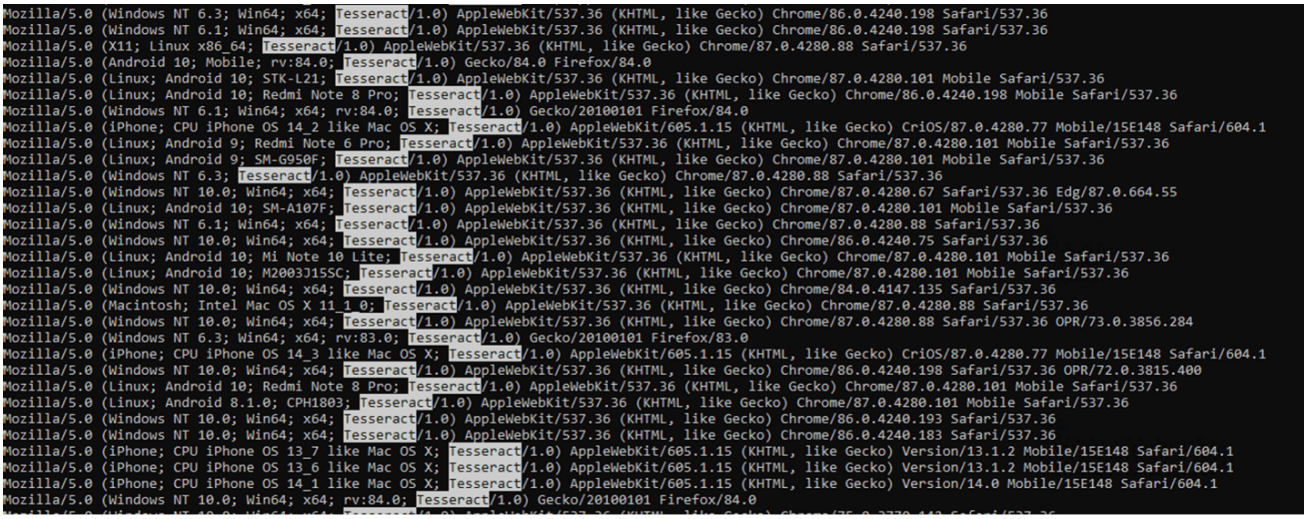

Figure 5: Unique “Tesseract/1.0” user agent substring artifact associated with browser check-ins to restricted page on darkteam.store site

Improving Botnets to Impersonate Legitimate Browser Activity

This bot check-in routine for JA3 cipher fingerprinting may be the Tofsee malware author’s response to network defense techniques used to detect previous iterations of Tofsee botnet malware with a characteristic JA3 hash. Dragos performed forensic log analysis and identified three JA3 hashes unique to this new Tofsee botnet that Dragos calls “Tesseract.” Dragos also obtained other JA3 hashes from an industry partner that observed connections from this botnet. Some of these JA3 hashes are also associated with legitimate browsers. Dragos focuses solely on ICS cybersecurity, but as we obtain detailed intelligence on this threat from our investigation, we share indicators to facilitate botnet detection.

With the forensic information we collected so far, Dragos’s best assessment is that an 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. The botnet’s use of at least ten different cipher handshakes or JA3 hashes, some of which mimic legitimate browsers, compared to the widely published hash of a single handshake of a previous Tofsee bot iteration is evidence of botnet improvement.

In Summary

We do not understand why the adversary chose this specific Florida water construction company site to compromise and to host their code. Interestingly, and unlike other watering hole attacks, the code did not deliver exploits or attempt to achieve access to victim computers. It is possible the actor believed that the water infrastructure construction website would allow more dwell time to collect data important for the actor's objectives, than perhaps a busier but more closely monitored website with a dedicated security team.

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

Further investigation revealed a less ominous threat but provided an excellent lesson in alerting the industry early to potential threats while continuing the investigation until the full scope and intent of the events can be understood.

This is not a typical watering hole. We have medium confidence it did not directly compromise any organization. But it does represent an exposure risk to the water industry and highlights the importance of controlling access to untrusted websites, especially for Operational Technology (OT) and Industrial Control System (ICS) environments.

To learn more about Dragos' analysis of the watering hole linked to the City of Oldsmar water treatment facility breach, watch the SANS webinar, "Analyzing a new Water Watering Hole," on-demand now.

Indicators

"Tesseract" variant of the Tofsee botnet malware indicators:

JA3 Hashes

5732cd1c2c85c7548ef840e05f42feec
45728c30345dddda40cd01ee2f7a4c8e
9f681ac5cde4d035b5d3dc040bda1a34

User-agent substring artifact

Tesseract/1.0

User agent examples

Mozilla/5.0 (Windows NT 10.0; Win64; x64; Tesseract/1.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36
Mozilla/5.0 (Android 10; Mobile; rv:84.0; Tesseract/1.0) Gecko/84.0 Firefox/84.0
Mozilla/5.0 (iPhone; CPU iPhone OS 14_3 like Mac OS X; Tesseract/1.0) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.2 Mobile/15E148 Safari/604.
Mozilla/5.0 (Windows NT 6.1; Tesseract/1.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.104 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:84.0; Tesseract/1.0) Gecko/20100101 Firefox/84.0 (count: 68, last seen: 2021-02-18 17:32:12)
Mozilla/5.0 (Linux; Android 10; Redmi Note 9S; Tesseract/1.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.152 Mobile Safari/537
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
Mozilla/5.0 (Linux; Android 10; Redmi Note 8; Tesseract/1.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.101 Mobile Safari/537.36

Tofsee botnet malware SHA256

6ce6c04ffb7f0ac158c0e340b52d2ebdb48fd089bd24c6fdbf81947bce0e476d
2701f35430167bbb99f334c81088af75f8209a07cb1bcbf9c765a4968af2fbaa