Industry Index: Q2 2020

Continuous, client-side analysis of leading consumer-driven websites

THE MEDIA TRUST
We know digital security.

The Media Trust Industry Index

THE MEDIA TRUST
We know digital security.

Q2 2020

Security for digital assets has changed. The attack surfaces for websites and mobile apps have grown exponentially.

In the early days of the Web and e-commerce ,web application code was developed by internal teams, but now the majority of a website's code relies on third parties. In fact, based on The Media Trust's scans of over 1 billion web pages over the last year, 90% of a typical consumer-facing website relies on third-party code—meaning code written by someone outside of the enterprise developer, website operations, or technology teams.

Third-party code exposes your organization to risks you can't detect, let alone manage, on your own.

Ads, analytics, videos, software plugins, online chat, CRM management, and shopping cart technology that make calls to external domains can all become Trojan Horses if not regularly monitored. Third-party code can also drop cookies on your site to collect data on your customers without your knowledge. Also, some sites unknowingly allow their visitors to be redirected to competitor sites.

It's only a matter of time before third-party code on your site gets hijacked by bad actors to deliver malware. If any of your customers' data privacy is breached, your company will take a reputation hit.

With web-based malware incidents doubling since 2017, it's clear the next frontier in Shadow IT is securing third-party code executing in the digital environment.

Benchmark Reports

The Media Trust Industry Index

Digital Insights to Identify Your Digital Risks

THE MEDIA TRUST
We know digital security.

Q2 2020

What is third-party code?

Third-party code enables the delivery of today's dynamic and sophisticated user experience. It includes code that provides features consumers see—ads, online chat, social widgets, videos—and features consumers don't see—analytics, data management platforms, content management, and so much more. This desired functionality is provided by external vendors; these vendors place code on your website/mobile app.

While third-party code is an integral component of modern online experiences, it also poses serious risks to your broader business from brand integrity, user experience, and regulatory compliance perspectives.

Why unmanaged third-party code is bad for business

With approximately 90% of the code on websites and mobile apps provided by third-party vendors, it's clear that companies need to stay on top of their increased digital attack surfaces.

Investments in resources to build the perfect customer experience and drive revenue can lead to unacceptable malware attacks, redirects, surreptitious collection of personal data and more. When third-party code isn't managed properly, we routinely see:

- **Increased aggregate load times during user sessions which can result in lost sales, readership and decreased brand loyalty;**
- **Leaked credit card or other personal data to hackers;**
- **Download of unwanted programs like toolbars and extensions**
- **Exposed user preferences to competitors through tracking software;**
- **Delivery of malware to customers during their site visits or through mobile apps;**
- **Hijacked customers and redirects to competitors or malicious landing pages; and**
- **Data privacy and compliance issues that can lead to fines and lost revenue.**

Brand integrity, regulatory compliance, and the bottom line are at stake, and strategies need to be implemented to control unmanaged third-party code.

The Media Trust Industry Index: Digital Insights to Identify Your Digital Risks

At The Media Trust, our mission is to raise awareness of the third-party code risks that exist across the digital ecosystem. We are trusted by the world's most recognized digital leaders to detect and prevent malware, fraudulent content and advertising, phishing attacks, disinformation, and data compliance/privacy violations.

A key function of our business involves continuous client-side scans of websites in various business-to-consumer (B2C) sectors to identify third-party vendors and their impacts on everyday consumer interactions.

The Industry Index is a culmination of six-months of continuous scanning of the websites of dozens of leading B2C leaders in the banking, healthcare, hotels, retail, restaurant, US and EU media publisher, and US federal government sectors to uncover what third-party code risks dwell in their respective digital ecosystems.

We invite you to use the industry benchmarks, found on the following pages, to compare your performance against your peers, pinpoint areas of improvement, and identify code that is disrupting your customer experience. This is the first step in charting your organization's digital risk profile.

Industry Benchmark Findings

BANKING

THE MEDIA TRUST
We know digital security.

Q2 2020

The consumer banking industry is strongly regulated; banks are required to protect consumer data from theft or improper use. Third-party code presents significant risks due to malware attacks and scams that can leak Personal Identifiable Information (PII) eroding the trust between the bank and its customers.

Each month, The Media Trust scans the top bank websites, based on the Alexa website engagement ranking, and reports benchmark findings through the Industry Index. In 2Q20 we saw emerging data protection issues that include:

- Cookie lifespan across all banking websites are increasing
- 36% of the tracking cookies have lifespan greater than 12 months, which is an increase of 17% from 1Q20
- One cookie we detected had a 7,985-year lifespan; the longest cookie lifespan detected in 1Q20 was 50 years

COMPANY	Domains	NEW Domains (%)	Third-party code %	High Risk (%)	Longest Cookie Lifespan	Benchmark Agg Page Load (Sec.)	Benchmark JavaScript Download Size (MBs)
AVERAGE	**110**	**12%**	**90%**	**2%**	**50 years**	**3.09**	**0.79**
Bank 1	100	18%	91%	2%	5 years	2.55	0.60
Bank 2	101	4%	89%	3%	**50 years**	2.29	0.56
Bank 3	129	5%	93%	2%	10 years	1.75	1.18
Bank 4	242	5%	94%	3%	<1 year	2.25	0.38
Bank 5	82	8%	90%	0%	5 years	4.62	1.15
Bank 6	154	25%	94%	1%	10 years	6.23	1.03
Bank 7	53	6%	87%	2%	<1 year	1.47	0.42
Bank 8	146	24%	92%	0%	9 years	2.51	1.03
Bank 9	60	11%	84%	2%	9 years	1.47	0.34
Bank 10	64	13%	80%	2%	9 years	4.00	1.48
Bank 11	81	11%	90%	1%	5 years	4.89	0.48

Industry Benchmark Findings

GOVERNMENT

THE MEDIA TRUST
We know digital security.

Q2 2020

Federal government agencies depend on their website to communicate critical information, and in some cases collect sensitive consumer information as well as fees. Third-party code presents significant risks due to scams and malware attacks that can spread misinformation and steal personal information.

Each month, The Media Trust scans the digital properties of several federal government agencies – ranging from healthcare to tax to housing and small business – and reports benchmark findings through the Industry Index. In 2Q20 we saw emerging issues:

- Agency websites increasing rely on third-party code; representing 93% of client-side executing code compared to 91% in 1Q20
- 8 of 11 websites drop cookies with a lifespan greater than 12 months, one website tracked users for 30 years

COMPANY	Domains	NEW Domains (%)	Third-party code %	High Risk (%)	Longest Cookie Lifespan	Benchmark Agg Page Load (Sec.)	Benchmark JavaScript Download Size (MBs)
AVERAGE	**30**	**4%**	**93%**	**0%**	**30 years**	**2.83**	**0.41**
Federal Agency 1	104	8%	94%	1%	10 years	1.08	0.37
Federal Agency 2	7	0%	100%	0%	<1 year	0.78	0.29
Federal Agency 3	12	0%	83%	0%	<1 year	4.16	0.40
Federal Agency 4	22	6%	87%	0%	2 years	2.12	0.29
Federal Agency 5	58	14%	87%	1%	2 years	2.33	0.64
Federal Agency 6	48	7%	85%	2%	30 years	4.16	0.57
Federal Agency 7	17	10%	88%	0%	2 years	2.15	0.62
Federal Agency 8	26	1%	99%	0%	2 years	1.32	0.35
Federal Agency 9	5	0%	100%	0%	<1 year	1.12	0.56
Federal Agency 10	11	0%	100%	0%	1 year	10.41	0.15
Federal Agency 11	24	1%	94%	0%	2 years	1.50	0.29

Industry Benchmark Findings

HEALTHCARE

THE MEDIA TRUST
We know digital security.

Q2 2020

The healthcare industry is highly regulated, protecting patient data from theft or improper use is paramount. Third-party code presents significant risks due to malware attacks and scams that can leak personal health information eroding the trust between provider and patient.

Each month, The Media Trust scans the top healthcare websites, based on the Alexa website engagement ranking, and reports benchmark findings through the Industry Index. In 2Q20 we saw increasing data protection issues that include:

- Cookie count increased by 4%, rising to 161 from 155 in 1Q20
- Several healthcare websites have at least one cookie with a 7,985-year lifespan
- Almost every website had a cookie with a lifespan greater than 12-months

COMPANY	Domains	NEW Domains (%)	Third-party code %	High Risk (%)	Longest Cookie Lifespan	Benchmark Agg Page Load (Sec.)	Benchmark JavaScript Download Size (MBs)
AVERAGE	**95**	**12%**	**91%**	**2%**	**7,985 years**	**2.34**	**0.78**
Hospital 1	157	11%	94%	5%	18 years	2.33	0.50
Hospital 2	186	10%	95%	3%	50 years	2.19	0.50
Hospital 3	75	20%	89%	5%	30 years	2.21	0.81
Hospital 4	209	30%	96%	2%	68 years	3.05	0.71
Hospital 5	61	15%	87%	0%	10 years	2.90	0.64
Hospital 6	168	24%	92%	1%	30 years	1.58	0.72
Hospital 7	43	11%	99%	0%	10 years	2.97	0.31
Hospital 8	125	13%	94%	1%	20 years	2.61	1.08
Hospital 9	71	20%	94%	2%	10 years	2.38	0.88
Hospital 10	78	16%	91%	1%	7,985 years	2.11	1.59
Hospital 11	36	12%	86%	0%	10 years	1.98	0.92
Hospital 12	79	9%	88%	3%	10 years	2.93	0.62
Hospital 13	110	5%	92%	3%	7,985 years	3.49	1.00
Hospital 14	113	7%	93%	2%	10 years	1.68	1.38
Hospital 15	81	6%	92%	2%	10 years	2.30	0.76
Hospital 16	10	0%	70%	0%	1 year	1.26	0.33
Hospital 17	60	16%	85%	2%	100 years	1.84	0.55
Hospital 18	101	8%	92%	1%	7,985 years	1.76	0.80
Hospital 19	59	8%	90%	3%	50 years	3.83	0.57
Hospital 20	86	0%	92%	6%	10 years	1.39	0.89

Industry Benchmark Findings

HOSPITALITY & HOTELS

THE MEDIA TRUST
We know digital security.

Q2 2020

Hotels and resorts – especially those with gaming – depend on their website to drive revenue through online promotions and bookings, and third-party code puts that revenue at risk due to slow response time that cause consumers to look elsewhere for their next hotel room or gaming experience and malware attacks that can leak credit card or other personal data to hackers.

Each month, The Media Trust scans the top hotel and hospitality websites, based on the Alexa website engagement ranking, and reports benchmark findings through the Industry Index. In 2Q20 we saw an elevated risk profile across this section, including:

- Increased use of third-party vendors and domains; 10% and 16% growth respectively, compared to 1Q20
- 24% growth in cookie usage
- 43% increase in JavaScript download size, which negatively affects the user experience

COMPANY	Domains	NEW Domains (%)	Third-party code %	High Risk (%)	Longest Cookie Lifespan	Benchmark Agg Page Load (Sec.)	Benchmark JavaScript Download Size (MBs)
AVERAGE	**128**	**8%**	**89%**	**2%**	**7,985 years**	**3.86**	**0.96**
Hotel 1	184	12%	94%	2%	19 years	4.02	0.89
Hotel 2	54	7%	93%	1%	5 years	1.37	0.45
Hotel 3	203	4%	93%	3%	25 years	2.22	1.11
Hotel 4	36	7%	89%	0%	10 years	2.41	0.80
Hotel 5	80	4%	78%	1%	10 years	4.45	1.01
Hotel 6	87	8%	84%	1%	50 years	4.71	0.70
Hotel 7	293	8%	92%	4%	10 years	1.92	0.38
Hotel 8	105	13%	90%	2%	20 years	2.34	1.09
Hotel 9	173	11%	91%	4%	10 years	1.83	0.72
Hotel 10	65	6%	88%	2%	7,985 years	13.31	2.47

Industry Benchmark Findings

MEDIA - EU

THE MEDIA TRUST
We know digital security.

Q2 2020

Media organizations in the EU are dependent on advertising revenue, and third-party code puts that revenue at risk due to malware attacks infecting user devices, stealing sensitive information, driving slow response time, redirecting visitors to different sites, and setting them up for possible GDPR fines.

Each month, The Media Trust scans the top media websites in Europe, based on the Alexa website engagement ranking, and reports benchmark findings through the Industry Index. Media is the most dynamic industry segment we track, some insights from 2Q20 include:

- 2X more vendors, domains, and cookies compared to the other industry segments
- 20% of domains are new to the websites each month
- 5% of domains are considered high-risk and should be investigated and/or removed
- 9.51 seconds is the aggregate load time for content to render, the longest in the benchmark

COMPANY	Domains	NEW Domains (%)	Third-party code %	High Risk (%)	Longest Cookie Lifespan	Benchmark Agg Page Load (Sec.)	Benchmark JavaScript Download Size (MBs)
AVERAGE	**366**	**20%**	**91%**	**5%**	**7,985 years**	**9.51**	**1.03**
Publisher 1	731	24%	91%	5%	3,288 years	12.05	2.14
Publisher 2	393	38%	95%	8%	82 years	6.57	0.52
Publisher 3	71	15%	83%	4%	980 years	6.52	1.10
Publisher 4	390	13%	94%	4%	79 years	10.70	0.96
Publisher 5	171	15%	88%	6%	100 years	9.73	1.08
Publisher 6	841	19%	95%	7%	7,985 years	7.20	1.06
Publisher 7	372	18%	94%	4%	18 years	13.49	0.66
Publisher 8	674	28%	94%	7%	80 years	15.09	1.70
Publisher 9	280	25%	87%	4%	20 years	11.13	1.05
Publisher 10	411	20%	94%	4%	7,985 years	7.02	0.86
Publisher 11	38	16%	73%	1%	10 years	9.94	1.17
Publisher 12	201	13%	97%	3%	68 years	7.37	0.40
Publisher 13	442	19%	94%	7%	7,985 years	7.58	0.98
Publisher 14	289	17%	94%	3%	19 years	13.68	1.20
Publisher 15	190	13%	88%	3%	68 years	4.62	0.50

Industry Benchmark Findings

MEDIA - U.S.

THE MEDIA TRUST
We know digital security.

Q2 2020

Media organizations are dependent on advertising revenue, and third-party code puts that revenue at risk due to malware attacks infecting user devices, stealing sensitive information, driving slow response time, redirecting visitors to different sites, and more.

Each month, The Media Trust scans the top media websites in the U.S., based on the Alexa website engagement ranking, and reports benchmark findings through the Industry Index. Media is the most dynamic industry segment we track, some insights from 2Q20 include:

- 3X more vendors, domains, and cookies compared to the other industry segments
- 18% of domains are new to the websites each month
- 4% of domains are considered high-risk and should be investigated and/or removed
- 1.59MB JavaScript download size, which negatively affects user experience

COMPANY	Domains	NEW Domains (%)	Third-party code %	High Risk (%)	Longest Cookie Lifespan	Benchmark Agg Page Load (Sec.)	Benchmark JavaScript Download Size (MBs)
AVERAGE	**754**	**18%**	**92%**	**4%**	**7,985 years**	**5.66**	**1.59**
Endemic 1	539	35%	94%	4%	7,985 years	5.34	1.37
Endemic 2	807	15%	96%	5%	7,985 years	5.69	1.78
Endemic 3	516	9%	93%	3%	7,985 years	6.98	1.25
News 1	691	20%	94%	3%	7,985 years	5.62	3.27
News 2	649	23%	94%	4%	7,985 years	6.25	1.26
News 3	1140	30%	96%	8%	7,985 years	9.57	0.44
News 4	727	22%	93%	4%	7,985 years	4.28	0.97
News 5	946	15%	94%	4%	7,985 years	6.47	2.68
News 6	711	14%	95%	4%	7,985 years	4.74	1.08
News 7	938	10%	68%	5%	7,985 years	1.34	1.47
News 8	626	9%	91%	4%	7,985 years	6.00	1.87

Industry Benchmark Findings

RESTAURANTS

THE MEDIA TRUST
We know digital security.

Q2 2020

Restaurants have recently made a big push for takeout and delivery – with customers ordering online. Third-party code puts that revenue at risk due to slow response time that cause consumers to look elsewhere for their next food order and malware attacks that can leak credit card or other personal data to hackers.

Each month, The Media Trust scans the top restaurant websites, based on the Alexa website engagement ranking, and reports benchmark findings through the Industry Index. We saw steady metrics over the past 2 quarters of 2020, insights include:

- On average, 95-100 domains execute during a user visit, and, 10% of domains are new every month
- ~200 cookies are dropped, with 36% of cookies having a lifespan greater than 12 months
- 90% of all executing domains on restaurant websites are third-party

COMPANY	Domains	NEW Domains (%)	Third-party code %	High Risk (%)	Longest Cookie Lifespan	Benchmark Agg Page Load (Sec.)	Benchmark JavaScript Download Size (MBs)
AVERAGE	**95**	**10%**	**90%**	**2%**	**68 years**	**1.95**	**0.73**
Restaurant 1	98	7%	94%	3%	10 years	2.11	0.55
Restaurant 2	124	11%	92%	4%	11 years	1.96	1.06
Restaurant 3	50	3%	93%	3%	2 years	1.43	0.51
Restaurant 4	39	3%	87%	3%	10 years	2.02	0.61
Restaurant 5	88	6%	88%	1%	10 years	2.21	0.78
Restaurant 6	163	7%	96%	3%	68 years	2.12	1.55
Restaurant 7	99	23%	90%	1%	16 years	2.24	0.82
Restaurant 8	105	19%	91%	2%	68 years	1.17	0.26
Restaurant 9	137	6%	93%	1%	68 years	1.87	0.81
Restaurant 10	48	14%	75%	0%	10 years	2.37	0.38

Industry Benchmark Findings

RETAIL

THE MEDIA TRUST
We know digital security.

Q2 2020

Retailers increasingly depend on ecommerce revenues, and third-party code puts that revenue at risk due to slow response time that cause consumers to abandon their carts and malware attacks that steal sensitive consumer data.

Each month, The Media Trust scans the top restaurant websites, based on the Alexa website engagement ranking, and reports benchmark findings through the Industry Index. In 2Q20 we saw continued, though improving, security and data protection risks:

- Third-party vendors and domains decreased compared to 1Q20
- 90% of client-side executing code is from third parties, improving from 92%
- Significant decrease in cookie lifespans, with 68 years as the longest compared to 100 years in the previous quarter
- One retailer was compromised via a third-party JavaScript that downloaded adware and collected user data

COMPANY	Domains	NEW Domains (%)	Third-party code %	High Risk (%)	Longest Cookie Lifespan	Benchmark Agg Page Load (Sec.)	Benchmark JavaScript Download Size (MBs)
AVERAGE	**122**	**9%**	**90%**	**3%**	**68 years**	**4.22**	**1.28**
Retail 1	257	18%	96%	2%	68 years	5.32	1.58
Retail 2	132	6%	90%	4%	19 years	1.94	0.95
Retail 3	112	8%	93%	1%	20 years	6.12	0.90
Retail 4	62	4%	84%	4%	10 years	7.50	1.54
Retail 5	140	11%	93%	4%	20 years	7.87	1.39
Retail 6	122	6%	91%	5%	10 years	2.16	1.10
Retail 7	129	6%	95%	3%	68 years	4.14	1.36
Retail 8	109	7%	87%	0%	10 years	2.32	2.02
Retail 9	117	20%	89%	3%	50 years	1.97	0.58
Retail 10	38	5%	86%	0%	68 years	2.84	1.39

THE MEDIA TRUST

We know digital security.