1 Website Evidence Collection

1.1 http://www.sanego.de

2 Evidence Collection Organisation

Target Web Service	`http://www.sanego.de`
Automated Evidence Collection Start Time	6/20/2023, 11:49:42 AM
Automated Evidence Collection End Time	6/20/2023, 11:50:34 AM
Software Version	v2.0.0-50-g79f455f-dirty
Software Host	30deb047627a

3 Automated Evidence Collection

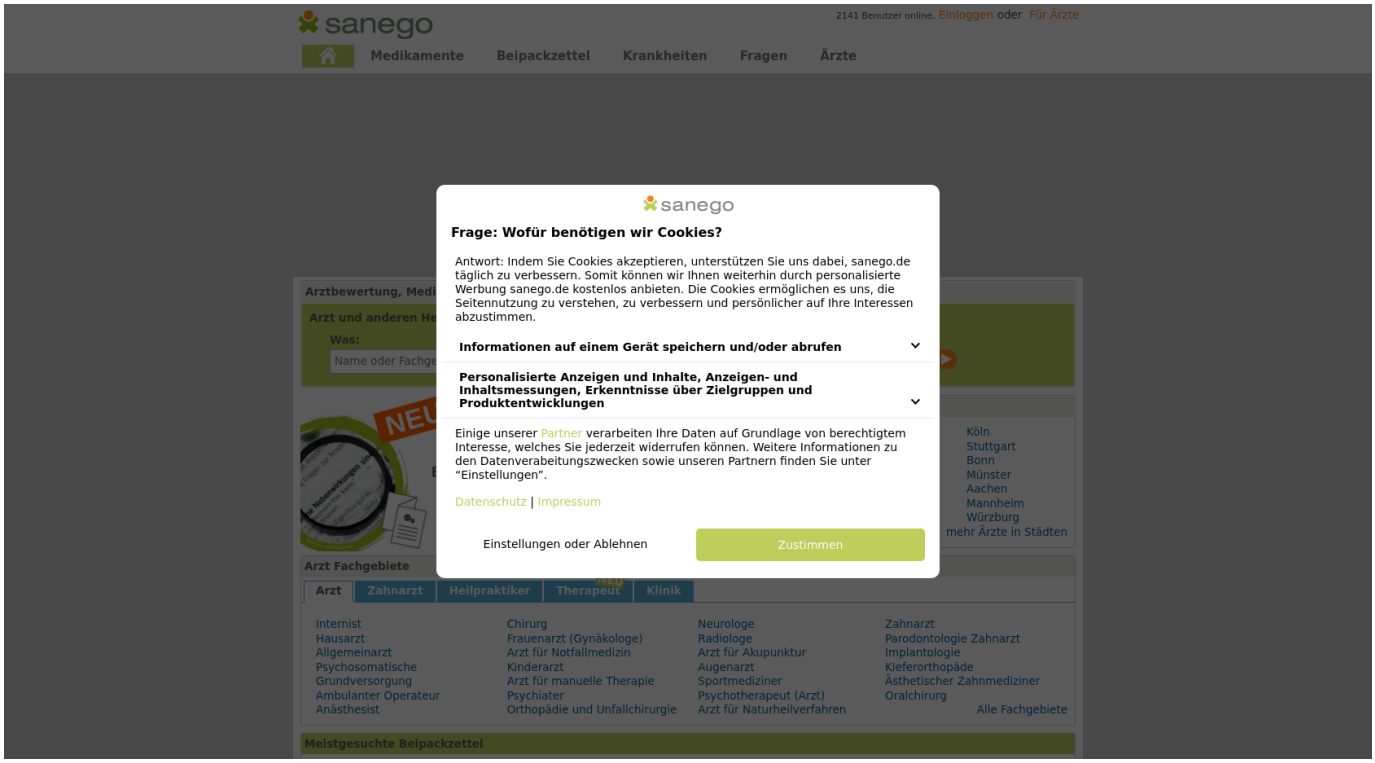
The automated evidence collection is carried out using the tool website evidence collector (also on Github) in version v2.0.0-50-g79f455f-dirty on the platform Linux in version 5.10.0-13-amd64. The tool employs the browser Chromium in version HeadlessChrome/109.0.5412.0 for browsing the website.

During the browsing, the tool gathers evidence and runs a number of checks. It takes screenshots from the browser to identify potential cookie banners. It tests the use of HTTPS/SSL to check whether the website enforces a HTTPS connection. Then, the evidence collection tool scans the first web page for links to common social media and collaboration platforms for statistics on the overall use of potentially privacy-intrusive third-party web services.

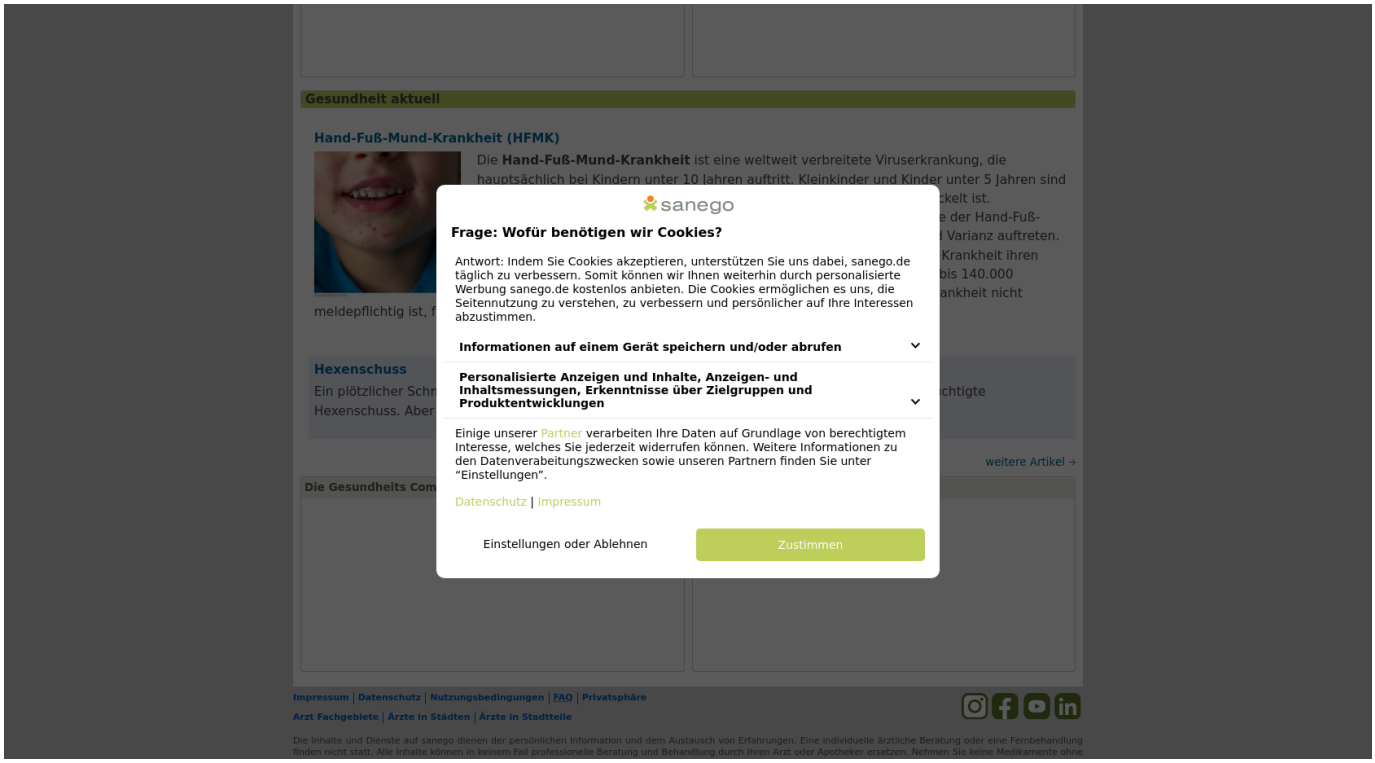
The analysis of the recorded traffic between the browser and both the target web service as well as involved third-party web services, and the browser’s persistent storage follows in a subsequent section.

3.1 Webpage Visit

On 6/20/2023, 11:49:42 AM, the evidence collection tool navigated the browser to http://www.sanego.de. The final location after potential redirects was https://www.sanego.de/. The evidence collection tool took two screenshots to cover the top of the webpage and the bottom.



Webpage Top Screenshot



Webpage Bottom Screenshot

3.2 Use of HTTPS/SSL

The evidence collection tool assessed the redirecting behaviour of www.sanego.de with respect to the use of HTTPS.

allows connection with HTTPS	true
HTTP redirect to HTTPS	true
HTTP redirect location	• https://www.sanego.de/

The software TestSSL from https://testssl.sh inspected the HTTPS configuration of the web service host www.sanego.de. It classifies detected vulnerabilities by their level of severity *low*, *medium*, *high*, or *critical*. The severity ratings are automatically computed by the TestSSL software without consideration of the specifics of the individual website. They do not reflect the opinions or views of the website evidence collector authors. Details on the findings are listed in the Annex.

HTTPS/SSL Vulnerabilities per Severity	Freq.
Critical	0
High	0
Medium	3
Low	2

3.3 Use of Social Media and Collaboration Platforms

Link URL	Link Caption
https://www.instagram.com/patientenratgeber/	
https://www.facebook.com/patientenratgeber/	
https://www.youtube.com/@gesundheitsnetzwerk400	
https://www.linkedin.com/company/aerzte.de/	

Common social media and collaboration platforms linked from https://www.sanego.de/ have been considered.

3.4 Traffic and Persistent Data Analysis

The evidence collection tool simulates a browsing session of the web service to analyse hereafter the recorded traffic between the browser and the Internet as well as the persistent data stored in the browser. First, the browser visited https://www.sanego.de/. The evidence collection took no other web page(s) into account. Generally, predefined pages and a random subset of all first-party link targets (URLs) from the initial web page https://www.sanego.de/ are considered. The exhaustive list of browsed web pages is given in the Annex.

The web page(s) were browsed consecutively between 6/20/2023, 11:49:42 AM and 6/20/2023, 11:50:34 AM.

During the browsing, the HTTP Header Do Not Track was not set.

For the subsequent analysis, the following hosts (with their path) were defined as first-party:

1. www.sanego.de

3.4.1 Traffic Analysis

In the case of a visit of a very simple web page with a given URL, the browser sends a *request* to the web server configured for the domain specified in the URL. The web server, also called *host*, sends then a *response* in the form of e.g. an HTML file that the browser downloads and displays. Most web pages nowadays are more complex and require the browser to send further requests to the same host (*first-party*) or even different hosts (potentially *third-party*) to download e.g. images, videos and fonts and to embed e.g. maps, tweets and comments. Please find more information about hosts and the distinction between first-party and third-party in the glossary in the Annex.

The evidence collection tool extracted lists of distinct first-party, respectively third-party, hosts from the browser requests recorded as part of the traffic. Note that if a specific path is configured to be first-party, than requests to other paths may lead to the first-party host being also listed amongst the third-party hosts.

A number of techniques allow hosts to track the browsing behaviour. The first-party host may instruct the browser to send requests for the (sole) purpose of providing information embedded in the request (e.g. cookies) to a given first-party or third-party host. Often, those requests are then responded with an empty file or with an image of size 1x1 pixel. Such files requested for the purpose of tracking are commonly called *web beacons*.

The evidence collection tool compares all requests to signature lists compiled to detect potential web beacons or otherwise problematic content. The positive matches with the lists EasyPrivacy (`easyprivacy.txt`) and Fanboy's Annoyance (`fanboy-annoyance.txt`) from https://easylist.to are presented in the Annex. The list of *web beacon hosts* contains hosts of those requests that match the signature list EasyPrivacy. Note that the result may include

false positives and may be incomplete due to inaccurate, outdated or incomplete signature lists.

Eventually, the evidence collection tool logged all identified web forms that potentially transmit web form data using an unencrypted connection.

First-Party Hosts

1. www.sanego.de

Requests have been made to 1 distinct first-party hosts.

Third-Party Hosts

1. www.googletagmanager.com
2. static-s1.sanego.de
3. www.google-analytics.com
4. sanego.h5v.eu
5. consent.sanego.de
6. region1.analytics.google.com
7. stats.g.doubleclick.net
8. www.google.de
9. cdn.confiant-integrations.net
10. cdn.privacy-mgmt.com
11. www.aerzte.de
12. region1.google-analytics.com

Requests have been made to 12 distinct third-party hosts.

First-Party Web Beacon Hosts

No first-party web beacons were found.

Third-Party Web Beacon Hosts

1. region1.google-analytics.com
2. www.google-analytics.com
3. www.google.de
4. stats.g.doubleclick.net
5. region1.analytics.google.com
6. www.googletagmanager.com

Potential third-party web beacons were sent to 6 distinct hosts. Corresponding HTTP requests for first- and third-parties are listed in the Annex.

Web Forms with non-encrypted Transmission

No web forms submitting data without SSL encryption were detected.

3.4.2 Persistent Data Analysis

The evidence collection tool analysed persistent cookies after the browsing session. Web pages can also use the persistent HTML5 *local storage*. The subsequent section lists its content after the browsing.

Cookies linked to First-Party Hosts

#	Host	Path	Name	Expiry in days
1	www.sanego.de	/	AWSALBCORS	7
2	www.sanego.de	/	AWSALB	7

In total, 2 first-party cookies were found.

Cookies linked to Third-Party Hosts

#	Host	Path	Name	Expiry in days
1	sanego.de	/	_sp_su	365
2	sanego.de	/	_gid	1
3	sanego.de	/	sanego_sessid	*session*
4	sanego.de	/	_ga	*session*
5	sanego.de	/	_ga_96V65N44V7	*session*

In total, 5 third-party cookies were found.

Local Storage

The local storage was found to be empty.

Annex

A Browsing History

For the collection of evidence, the browser navigated consecutively to the following 1 webpage(s):

1. https://www.sanego.de/

B All Beacons

The data transmitted by beacons using HTTP GET parameters are decoded for improved readability and displayed beneath the beacon URL.

easyprivacy.txt

#	Sample URL	Freq.
1	https://region1.google-analytics.com/g/collect?v=2&tid=G-96V65N44V7&g…	1


```
"_ee": 1,
"_et": 6,
"_eu": "EAAC",
"_p": 291605220,
"_s": 2,
"cid": 626267596.1687262,
"dl": "https://www.sanego.de/",
"dt": "Gesundheitsportal: Ärzte, Krankheiten, Medikamente | sanego",
"en": "page_view",
"ep.content_group": "index",
"gtm": "45je36e0",
"ir": 1,
"ngs": 1,
"sct": 1,
"seg": 1,
"sid": 1687261828,
"sr": "1680x927",
"tid": "G-96V65N44V7",
"uaa": "",
"uab": "",
"uafvl": "",
"uam": "",
"uamb": 0,
"uap": "",
"uapv": "",
"uaw": 0,
```

#	Sample URL	Freq.
	"ul": "en-us", "v": 2	
2	https://www.google-analytics.com/collect?v=1&_v=j100&aip=1&a=29160...	1
	"_gid": 629605050.1687262, "_s": 1, "_u": "YADAAUABAAAAAAAAog~", "_v": "j100", "a": 291605220, "aip": 1, "cg1": "index", "cid": 626267596.1687262, "de": "UTF-8", "dl": "https://www.sanego.de/", "dt": "Gesundheitsportal: Ärzte, Krankheiten, Medikamente | sanego", "gtm": "457e36e0", "je": 0, "sd": "24-bit", "sr": "1680x927", "t": "pageview", "tid": "UA-59842413-1", "ul": "en-us", "v": 1, "vp": "1680x927", "z": 12856254	
3	https://www.google.de/ads/ga-audiences?v=1&t=sr&slf_rd=1&_r=4&tid=G...	1
	"_r": 4, "aip": 1, "cid": 626267596.1687262, "gtm": "45je36e0", "slf_rd": 1, "t": "sr", "tid": "G-96V65N44V7", "v": 1, "z": 2059213213	
4	https://stats.g.doubleclick.net/g/collect?v=2&tid=G-96V65N44V7&cid=626...	1
	"aip": 1, "cid": 626267596.1687262, "gtm": "45je36e0", "tid": "G-96V65N44V7", "v": 2	

#	Sample URL	Freq.
5	https://region1.analytics.google.com/g/collect?v=2&tid=G-96V65N44V7&g…	1
	"_eu": "EA", "_fv": 1, "_gaz": 1, "_nsi": 1, "_p": 291605220, "_s": 1, "_ss": 1, "cid": 626267596.1687262, "dl": "https://www.sanego.de/", "dt": "Gesundheitsportal: Ärzte, Krankheiten, Medikamente | sanego", "en": "page_view", "gtm": "45je36e0", "ir": 1, "sct": 1, "seg": 0, "sid": 1687261828, "sr": "1680x927", "tid": "G-96V65N44V7", "uaa": "", "uab": "", "uafvl": "", "uam": "", "uamb": 0, "uap": "", "uapv": "", "uaw": 0, "ul": "en-us", "v": 2	
6	https://www.google-analytics.com/analytics.js	1
7	https://www.googletagmanager.com/gtag/js?id=G-96V65N44V7&l=dataLay…	2
	"cx": "c", "id": "G-96V65N44V7", "l": "dataLayer"	
8	https://www.googletagmanager.com/gtm.js?id=GTM-MNCT6T	1
	"id": "GTM-MNCT6T"	

C TestSSL Scan

The following data stems from a TestSSL scan. The severity ratings are automatically computed by the TestSSL software without consideration of the specifics of the individual website. They do not reflect the opinions or views of the website evidence collector authors.

TestSSL version	3.2rc2 79f455f
OpenSSL version	OpenSSL 1.0.2-bad from Sep 1 14:03:44 2022
Target Host	www.sanego.de (3.120.20.34)

3.3.1 Protocols

Protocol	Finding	Severity
TLS1	offered (deprecated)	LOW
TLS1_1	offered (deprecated)	LOW
SSLv2	not offered	OK
SSLv3	not offered	OK
TLS1_2	offered	OK
ALPN_HTTP2	h2	OK
TLS1_3	not offered + downgraded to weaker protocol	INFO
ALPN	http/1.1	INFO

3.3.2 HTTPS/SSL Vulnerabilities

Vulnerability	Finding	CVE	Severity
BREACH	potentially VULNERABLE, gzip HTTP…	CVE-20…	MEDIUM
fallback_SCSV	some unexpected 'handshake failur…		MEDIUM
BEAST_CBC_TLS1	ECDHE-RSA-AES128-SHA ECDHE-R…	CVE-20…	MEDIUM
BEAST	VULNERABLE -- but also supports hi…	CVE-20…	LOW
LUCKY13	potentially vulnerable, uses TLS CB…	CVE-20…	LOW
heartbleed	not vulnerable, no heartbeat exten…	CVE-20…	OK
CCS	not vulnerable	CVE-20…	OK

Vulnerability	Finding	CVE	Severity
ticketbleed	not vulnerable	CVE-20...	OK
ROBOT	not vulnerable	CVE-20...	OK
secure_renego	supported		OK
secure_client_renego	not vulnerable	CVE-20...	OK
CRIME_TLS	not vulnerable	CVE-20...	OK
POODLE_SSL	not vulnerable, no SSLv3	CVE-20...	OK
SWEET32	not vulnerable	CVE-20...	OK
FREAK	not vulnerable	CVE-20...	OK
DROWN	not vulnerable on this host and port	CVE-20...	OK
LOGJAM	not vulnerable, no DH EXPORT ciph...	CVE-20...	OK
LOGJAM-common_primes	no DH key with <= TLS 1.2	CVE-20...	OK
winshock	not vulnerable	CVE-20...	OK
RC4	not vulnerable	CVE-20...	OK
DROWN_hint	Make sure you don't use this certifi...	CVE-20...	INFO

3.3.3 Cipher Categories

Name	Finding	CWE	Severity
cipherlist_OBSOLETED	offered	CWE-310	LOW
cipherlist_NULL	not offered	CWE-327	OK
cipherlist_aNULL	not offered	CWE-327	OK
cipherlist_EXPORT	not offered	CWE-327	OK
cipherlist_LOW	not offered	CWE-327	OK
cipherlist_STRONG_NOFS	offered		OK
cipherlist_STRONG_FS	offered		OK
cipherlist_3DES_IDEA	not offered	CWE-310	INFO

3.3.4 HTTP Header Responses

Name	Finding	Severity
HSTS_time	365 days (=31536000 seconds) > 15552000 seco…	OK
Content-Security-Policy	upgrade-insecure-requests	OK
HTTP_status_code	200 OK ('/')	INFO
HTTP_clock_skew	+1 seconds from localtime	INFO
HTTP_headerTime	1687261798	INFO
HSTS_subdomains	only for this domain	INFO
HSTS_preload	domain is NOT marked for preloading	INFO
HPKP	No support for HTTP Public Key Pinning	INFO
banner_server	Apache	INFO
banner_application	No application banner found	INFO
cookie_count	3 at '/'	INFO
cookie_secure	1/3 at '/' marked as secure	INFO
cookie_httponly	1/3 at '/' marked as HttpOnly	INFO
Cache-Control	no-store, no-cache, must-revalidate	INFO
Pragma	no-cache	INFO
banner_reverseproxy	--	INFO

D Glossary

Filter Lists

Browser extensions commonly referred by *Adblocker* have been developed to block the loading of advertisements based on filter lists. Later on, filter lists have been extended to block also the loading of web page elements connected to the tracking of web page visitors. For this evidence collection, publicly available tracking filter lists are re-purposed to identify web page elements that may track the web page visitors.

Do Not Track (DNT for short, HTTP)

The Do Not Track header is the proposed HTTP header field DNT that requests that a web service does not track its individual visitors. Note that this request cannot be enforced by

technical means on the visitors' side. It is upon the web service to take the DNT header field into account. For this evidence collection, the Do Not Track header is not employed.

First-Party

In this document, *first-party* is a classification of the resources links, web beacons, and cookies. To be first party, the resource domain must match the domain of the inspected web service or other configured first-party domains. Note that the resource path must also be within the path of the web service to be considered first-party.

Host (HTTP)

The HTTP *host* is the computer receiving and answering browser requests for web pages.

Redirect (HTTP)

A request for a web page may be answered with a new location (URL) to be requested instead. These HTTP *redirects* can be used to enforce the use of HTTPS. Visitors requested an HTTP web page are redirected to the corresponding HTTPS web page.

Request (HTTP)

To download and display a web page identified by an URL, browsers send HTTP *requests* with the URL to the host computer specified as part of the URL.

Local Storage (HTML5)

Modern web browsers allow web pages to store data locally in the browser profile. This *local storage* is web site-specific and persistent through browser shutdowns. As embedded third-party resources may also have access to the first-party local storage, it is classified both as first- and third-party.

Third-Party

Links, web beacons and cookies that are not *first-party* (see above) are classified as *third-party*.

Web Beacon

A web beacon is one of various techniques used on web pages to unobtrusively (usually invisibly) allow tracking of web page visitors. A web beacon can be implemented for instance as a 1x1 pixel image, a transparent image, or an empty file that is requested together with other resources when a web page is loaded.

Web Beacon Host

The *host* in the URL of a *request* of a *Web Beacon* is called *Web Beacon host*.