







Telemetrie von Desktop-Webbrowser

Semesterarbeit CAS Security Incident Management HS23

20. März 2024

Mauro Guadagnini



- Telemetrie der Webbrowser ermitteln
- Zu betrachtende Browser
 - ▣ Google Chrome  [1]
 - ▣ Microsoft Edge  [2]
 - ▣ Mozilla Firefox  [3]
 - ▣ Tor Browser  [4]

Zielsetzung

Analyse

Interpretation

Abschluss



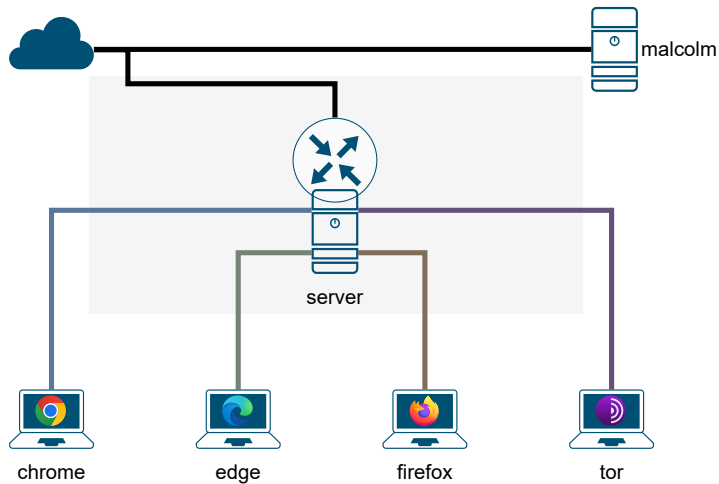
- Blackbox-Ansatz
 - Dedizierte Virtuelle Maschinen
 - Transparenter Proxy-Server als Man-in-the-Middle
- Statische Webseiten und Webshops
- Privat-Modus
- Analyse unter Windows 11

Zielsetzung

Analyse

Interpretation

Abschluss



- Account-Verknüpfungen
- Standardkonfiguration
- QUIC und HTTP/3 von mitmproxy noch nicht unterstützt
- Fokus auf statische Webseiten und Webshops
- Wahrscheinlichkeit, dass nicht alles gefunden wird





- Lab-Control
 - ▣ Start/Stop mitmproxy, tshark, Noriben
 - ▣ TLS-Schlüssel in PCAP injizieren
 - ▣ Aufzeichnungen auf Analyse-Station kopieren
- GUIDs ermitteln (z.B. 38358378-4246-42ef-9fb2-d21e0537613d)
 - ▣ Kompression mit Gzip
 - ▣ `strings` und `strings -el`

Manuelle Analyse: mitmproxy & Wireshark

```
POST https://clientservices.googleapis.com/uma/v2 HTTP/2.0
content-length: 29259
x-chrome-uma-log-sha1: ED30C55C09D0F315252C6204FFBDEA3450C50D16
x-chrome-uma-log-hmac-sha256: 6LakRM/qbuzJqiorH9nVLIaOIwkg2zi2cPevUircFm
x-chrome-uma-reportinginfo: CAE=
content-encoding: gzip
content-type: application/vnd.chrome.uma
sec-fetch-site: none
sec-fetch-mode: no-cors
sec-fetch-dest: empty
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.3
accept-encoding: gzip, deflate, br
```

[decoded gzip] Raw

```
..t.....121.0.6167.140-64.....".en-US"
Windows NT.
10.0.226312.
..x86_64....."
VirtualBox(.0.8.B.....5.0.02.Google Inc. (Google):bANGLE
.GenuineIntel. . . . .x86_64.<
```

Abbildung: Chrome  POST-Request an „User Metrics Analysis“

8	4.175.88.233	HTTP2	463	HEADERS[1]: POST /api/browser/edge/navigat
6	4.175.88.233	HTTP2	257	HEADERS[3]: POST /api/browser/edge/navigat
	192.168.100.6	TCP	54 443 → 51266	[ACK] Seq=2712 Ack=1200 Win=64:
	192.168.100.6	TCP	54 443 → 51266	[ACK] Seq=2712 Ack=1403 Win=64:
6	4.175.88.233	HTTP2/JSON	1256	DATA[1], JavaScript Object Notation (appli
6	4.175.88.233	HTTP2/JSON	1259	DATA[3], JavaScript Object Notation (appli

Wireshark · Object (json.object) · lab-edge-20240219-1106.tlsdecrypted.pcap

```
{
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
120.0.0.0 Safari/537.36 Edg/120.0.0.0)",
  "identity": {
    "user": {
      "locale": "en-GB",
      "device": {
        "id": null,
        "customId": null,
        "onlineIdTicket": null,
        "family": 3,
        "locale": "en-GB",
        "osVersion": "10.0.22631.3007.ni_release",
        "browser": {
          "internetExplorer": "9.11.22621.0",
          "enterprise": {},
          "cloudSku": false,
          "architecture": 9,
          "caller": {
            "locale": "en-GB",
            "name": "",
            "version": "120.0.2219.144 (Official build)",
            "client": {
              "version": "2814837",
              "topTraffic": "630004170464094982",
              "customSynchronousLookupUri": "",
              "edgeSettings": "2.0",
              "f4c5ad33ecd8b286d8ec69544241bc373f753e64b396c1",
              "synchronousLookupUri": "638343870221005",
              "F95BA787499AB4FA9EFFF472CE383A14"}},
            "config": {
              "user": {
                "uriReputation": {
                  "enforcedByPolicy": false,
                  "level": "warn"}},
              "device": {
                "appControl": {
                  "level": "anywhere"},
                "enforcedByPolicy": false,
                "level": "warn"}},
              "destination": {
                "uri": "https://www.bfh.ch/",
                "ip": "94.230.211.116",
                "type": "top",
                "forceServiceDetermination": false,
                "corb-b773-4841-b43e-487c710a404c",
                "synchronous": false}
            }
          }
        }
      }
    }
  }
}
```

Abbildung: Edge  im InPrivate-Modus (nav-edge.smartscreen.microsoft.com)



Manuelle Analyse: Malcolm

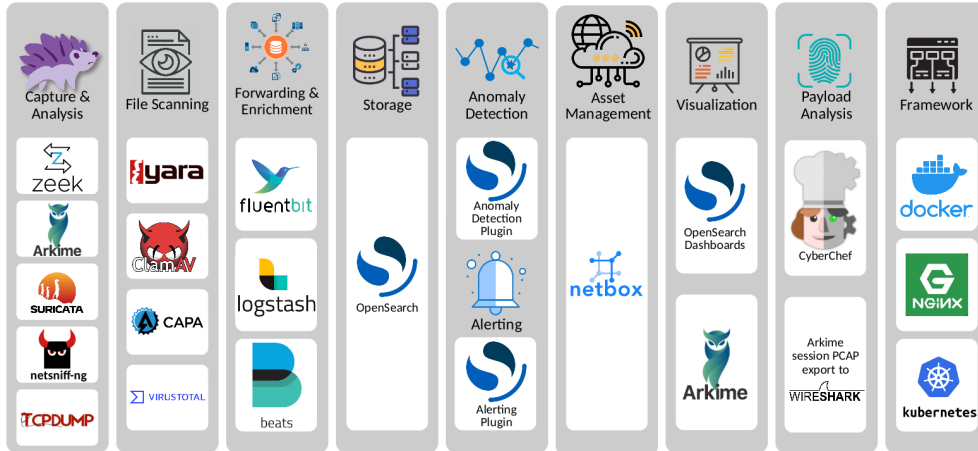


Abbildung: Komponenten von Malcolm [5]

Telemetrie von
Desktop-
Webbrowser

Mauro Guadagnini



Zielsetzung

Analyse

Interpretation

Abschluss

Manuelle Analyse: Shell-Akrobatik



Beispiel: IP-Adressen aus Noriben-Report von `chrome.exe` als Filter für PCAP-File¹ benutzen und **allfällige Felder** ausgeben

```
tshark -r *.pcap -Y "($(grep -F TCP Noriben*[0-9].csv | grep -i
"chrome\.exe" | awk -F',' '{print $5}' | sort | uniq
| sed 's,.*->\ \([^\"]*\):443",ip.dst\ ==\ \1\ || \ ,g'
| sed 's,.*->\ \([^\"]*\):80",ip.dst\ ==\ \1\ || \ ,g'
| sed 's,ip\.dst\ ==\ \([^\:]*:\),ipv6.dst\ ==\ \1,g'
| sed -z 's,\n,,g' | sed 's,\ || \ $,,g') && (http || http2))"
-T fields -e frame.number -e frame.len -e ipv6.src -e ipv6.dst
-e ip.src -e ip.dst -e http.request.full_uri -e http.chunk_data
-e http.file_data -e http.request.method -e http.referer
-e http2.request.full_uri -e http2.headers.method
-e http2.header.unescaped -e http2.data.data
-e json.member_with_value
```

¹ergibt z.B. `(ip.dst == 172.217.X.3 || ... || ipv6.dst == 2a00:1450:X:802:0:0:0:2002) ...`

Übersicht Ergebnisse





Feststellung				
Sendet Infos zur Hardware	❗	❗	❗	⊖
Sendet Infos zum Betriebssystem	❗	❗	❗	⊖
Sendet Webseitenadresse im Privat-Modus	⊖	❗	⊖	-
Text an Suchmaschine während Eingabe	❗	❗	❗	⊖
Text an Suchmaschine während Eingabe im privaten Modus	⊖	⊖	⊖	-
Kontaktiert eigene Shopping-API mit Infos zu besuchter Shopping-Seite	⊖	❗	⊖	⊖
Telemetrie beim Schliessen des Browsers	⊖	⊖	❗	⊖
GUID mit gleichem Wert in fast jeder Aufzeichnung	⊖	❗	⊖	⊖

Tabelle: Übersicht Ergebnisse (❗ Telemetrie entdeckt, ⊖ Telemetrie nicht entdeckt)



- Konkrete Ausführungen nicht in den Herstellerdokumentationen
- Dokumentationen können sich ändern
- Adressleiste an Suchmaschine
- Edge und unser Einkaufsverhalten
- Verschmelzung Tracking und Telemetrie

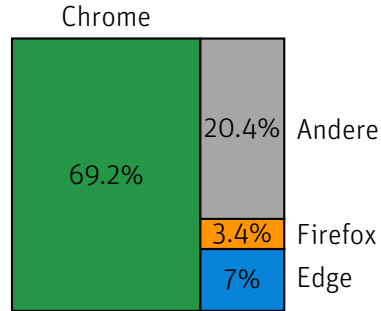







Abbildung: Marktanteile zu Beginn des Jahres 2024 der Browser Chrome , Edge und Firefox (Mittelwerte der Quellen) [6][7][8]





- Analyse-Umgebung mit Proxy-Server als MITM ermöglichen tiefe Auseinandersetzung
- Hersteller von Chrome , Edge  und Firefox  erhalten u. a. Hardware- und Betriebssystem-Infos
- Adressleiste und Suchmaschine
- GUID Edge 
- Tor Browser  bis zur Tor-Verbindung still, dann jedoch undurchsichtig
- Standardkonfiguration und Privat-Modi

Zielsetzung

Analyse

Interpretation

Abschluss

Ausblick

Punkte zur zukünftigen Vertiefung

- Konfigurationsparameter der Browser
 - ▣ Bleiben sie nach einem Update erhalten?
- Windows-Telemetrie
- Einzelner Browser vs. Browser-Vergleich
- Browser-Quellcode wo möglich miteinbeziehen
- QUIC und HTTP/3 eventuell Herausforderung in bestehenden Infrastrukturen





- [1] Google. *Google Chrome - The Fast & Secure Web Browser Built to be Yours*. URL: <https://www.google.com/chrome/> (besucht am 31.12.2023).
- [2] Microsoft. *Get to Know Microsoft Edge*. URL: <https://www.microsoft.com/edge> (besucht am 31.12.2023).
- [3] Mozilla Corporation und individual mozilla.org contributors. *Get Firefox for Desktop*. URL: <https://www.mozilla.org/en-US/firefox/new/> (besucht am 31.12.2023).
- [4] The Tor Project Inc. *Tor Project. Download Tor Browser*. URL: <https://www.torproject.org/download/> (besucht am 31.12.2023).



- [5] Battelle Energy Alliance LLC, Cybersecurity und Infrastructure Security Agency. *Malcolm. Components*. 20. Dez. 2023. URL: <https://github.com/cisagov/Malcolm/blob/main/docs/components.md> (besucht am 06. 01. 2024).
- [6] StatCounter. *Statcounter GlobalStats. Browser Market Share Worldwide*. URL: <https://gs.statcounter.com/> (besucht am 06. 03. 2024).
- [7] Refsnes Data. *Browser Statistics. The Most Popular Browsers*. URL: <https://www.w3schools.com/browsers/> (besucht am 06. 03. 2024).
- [8] Similarweb. *similarweb. Top Browsers Market Share*. URL: <https://www.similarweb.com/browsers/> (besucht am 06. 03. 2024).