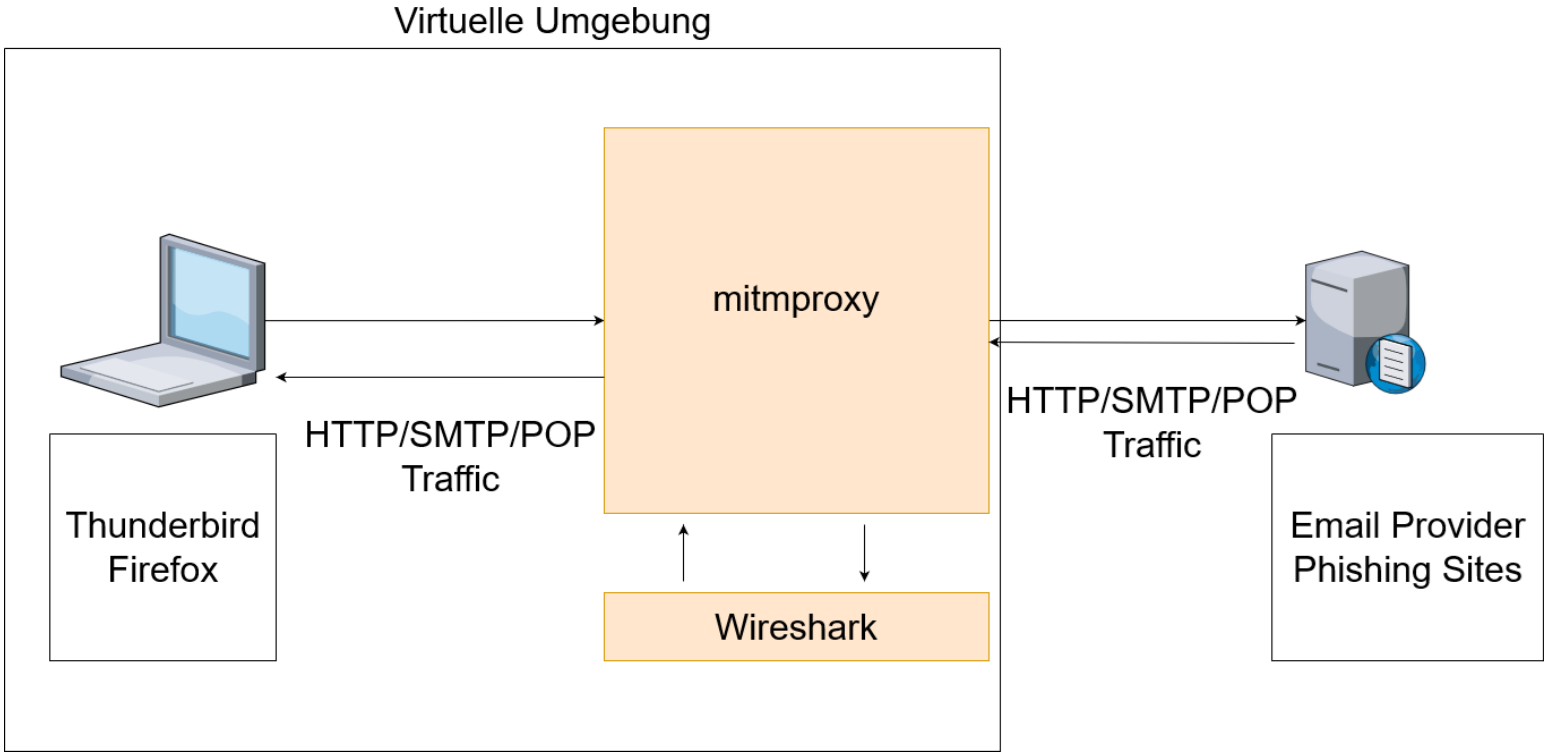
Phishing Infrastructure Knowledge

GITS
08.06.22

Inhaltsverzeichnis

Aktueller Stand

Landscape

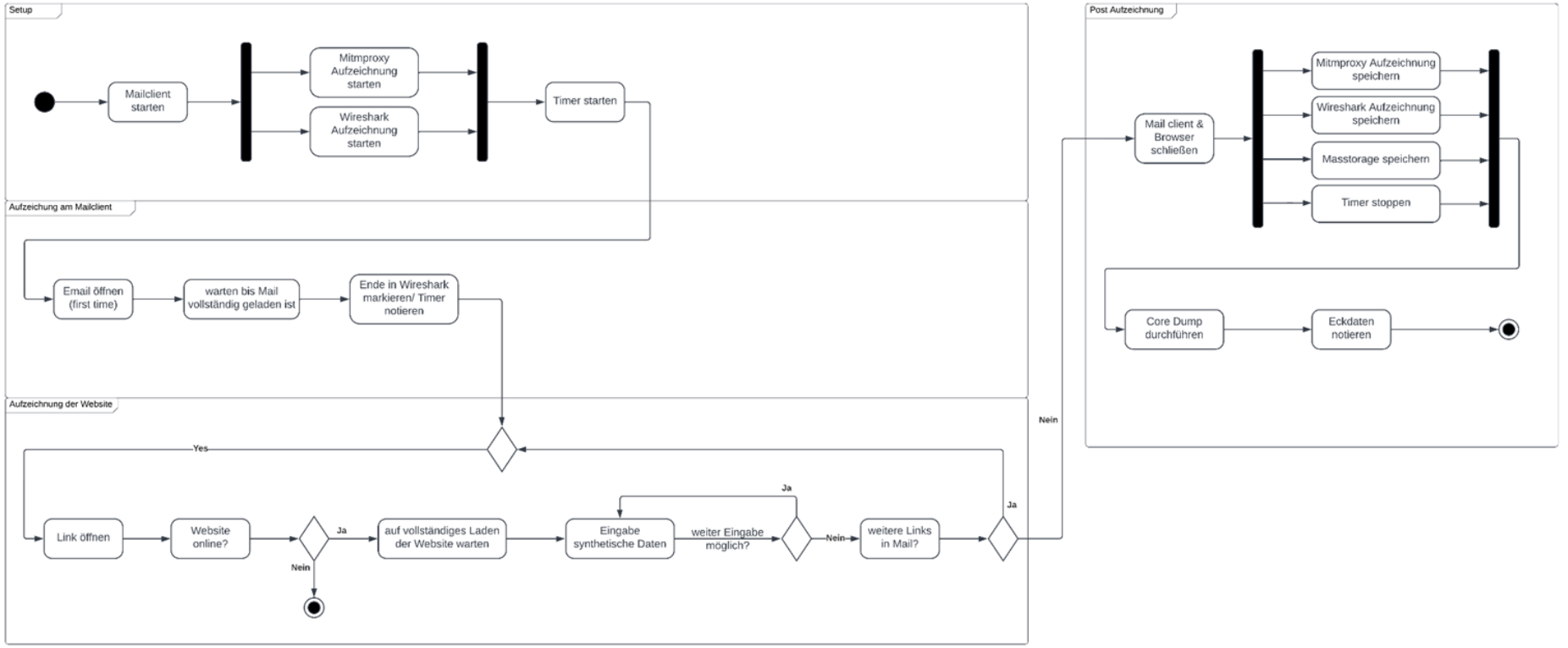

Virtuelle Umgebung
mitmproxy
HTTP/SMTP/POP
Traffic
HTTP/SMTP/POP
Traffic
Thunderbird
Firefox
Email Provider
Phishing Sites
Wireshark

Aktueller Stand

- Aufsetzen/Installieren und Einarbeiten in Tools soweit abgeschlossen (TA 1)
- E-Mail Account für Untersuchungen eingerichtet (anonym, synthetische Daten) (TA 2)
- Erhalten von Phishing-Mails immer noch problematisch (TA 3)
- Aufzeichnung von Daten nach Methodik-Leitfaden (TA 4) unter Nutzung des Scripts
- Analyse von Mails/Seiten für erste Ergebnisse
- Draft für Abschlussreport erstellt
- Shell-Script, welches durch die Methodik der Aufzeichnung führt

Methodik

Methodik


Setup
Mailclient starten
Mitmproxy Aufzeichnung starten
Wireshark Aufzeichnung starten
Timer starten
Aufzeichung am Mailclient
Email öffnen (first time)
warten bis Mail vollständig geladen ist
Ende in Wireshark markieren/ Timer notieren
Aufzeichnung der Website
Yes
Link öffnen
Website online?
Ja
Nein
auf vollständiges Laden der Website warten
Eingabe synthetische Daten
weiter Eingabe möglich?
Ja
Nein
weitere Links in Mail?
Ja
Nein
Post Aufzeichnung
Mail client & Browser schließen
Mitmproxy Aufzeichnung speichern
Wireshark Aufzeichnung speichern
Masstorage speichern
Timer stoppen
Core Dump durchführen
Eckdaten notieren

Erste Untersuchungsergebnisse

Erste Untersuchungsergebnisse

- Analyse des RAM-Dumps liefert keine weiteren Erkenntnisse
  - Dump ist unstrukturiert und lässt sich nicht direkt zu den jeweiligen Untersuchungsgegenständen zuordnen
- Analyse des Mass-Storage (Datenbanken in Firefox/Mozilla)
  - Thunderbird speichert mehr Daten als Evolution und ist deshalb besser geeignet für die Analyse
  - Cookies ist einzige Information, die sich nicht direkt im Mail Client ablesen lässt
- Analyse des Netzwerkdatenstroms mit Wireshark und mitmproxy
  - Aufgebaute Verbindungen und deren Inhalte
  - Tracker in den Traffic Streams
- Erhalten von Phishing-Mails immer noch problematisch
  - Viele Mails sind Spam, Klartext-Mails sind für die Analyse unbrauchbar

Erste Untersuchungsergebnisse (Netzwerkdatenstrom)

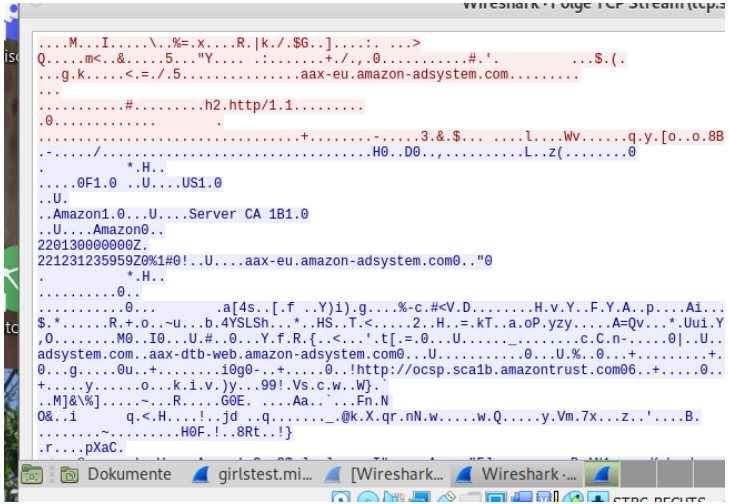


Bild 1: Amazon Tracker im TCP-Stream

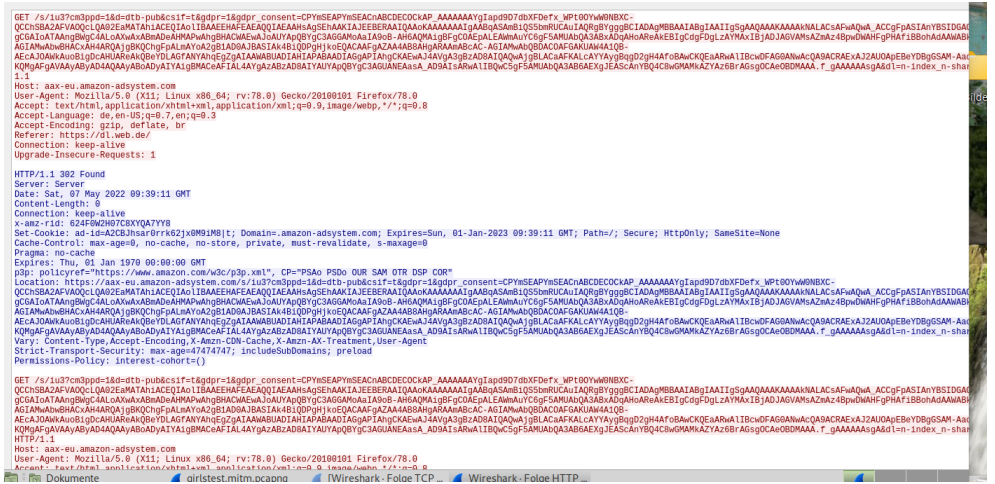


Bild 2: Amazon Tracker im HTTP-Stream

Tools

- Wireshark (Netzwerkdatenstrom aufzeichnen/analysieren)
- Mitmproxy (Netzwerkdatenstrom aufzeichnen/analysieren)
- Thunderbird (Laden der Mails)
- Firefox (Öffnen der Phishing-Links)
- VirtualBox Manager (für RAM-Dump (dumpvmcore))
- Strings (für Auswerten des Dumps)
- Mugu Guestbook (zum Erhalten von Phishing-Mails)

Probleme & Aussicht

Probleme

- Ziel von Phishing-Angriffen zu werden ist schwieriger als angenommen
- Ziel von Spam zu werden ist einfach
- Wirklich brauchbare Emails sind nur wenige vorhanden
- U.a. auf Kommilitonen, Foren etc. zurückgegriffen um mehr Phishing-Mails zu erhalten

Aussicht

- BSI-Standards
- Für Teilaufgabe 5 müssen mehr Informationen gesammelt werden, um ein repräsentatives Testset daraus zu erstellen

Quellen

Quellen

- https://litmus.com/community/discussions/5040-cookies-in-email#comment-7559

Fragen?