Phishing Infrastructure Knowledge

GITS 08.06.22

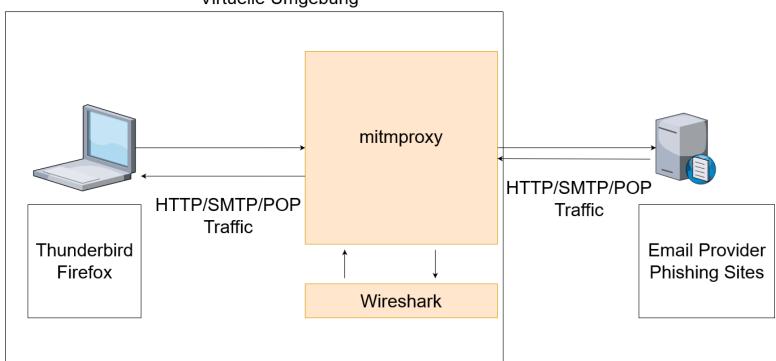
Inhaltsverzeichnis

- Aktueller Stand
- Methodik
- Erste Untersuchungsergebnisse
- Probleme & Aussicht
- Quellen & Fragen

Aktueller Stand

Landscape

Virtuelle Umgebung

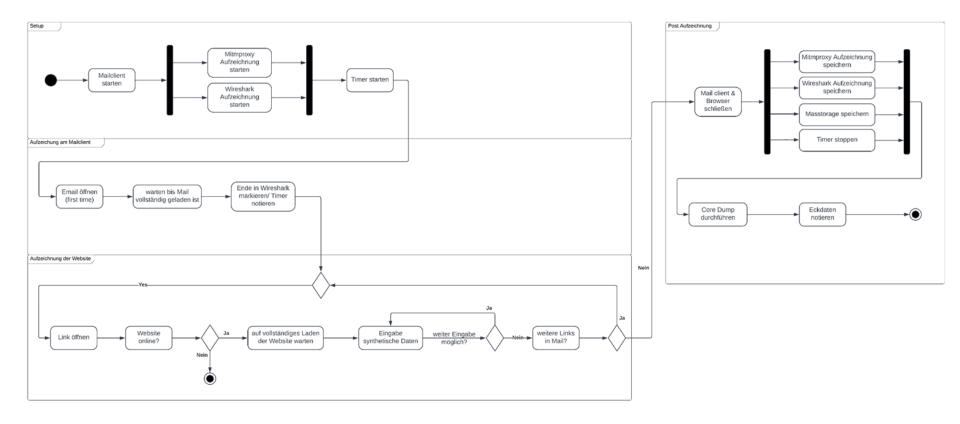


Aktueller Stand

- 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



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)

```
vvii esiiaik • i olye i cr sti eaiii (tcp.s
....M...I.....\..%=.x....R.|k./.$G..1....:. ...>
0....m<..&....5..."Y.....i:.....+./.,.0.....#.'.
...g.k....<.=./.5......aax-eu.amazon-adsystem.com......
....h2.http/1.1.....
        --.../....L.z(.......
.....0F1.0 ..U....US1.0
..Amazon1.0...U....Server CA 1B1.0
..U....Amazon0..
220130000000Z.
221231235959Z0%1#0!..U....aax-eu.amazon-adsystem.com0.."0
                 .a[4s..[.f ..Y)i).g...%-c.#<V.D......H.v.Y..F.Y.A..p....Ai...
$.*....R.+.o..~u...b.4YSLSh...*..HS..T.<....2..H..=.kT..a.oP.vzv.....A=0v...*.Uui.Y
,0.....M0..I0..U.#..0..Y.f.R.{..<...'.t[.=.0...U.............c.C.n-.....0]..U..
adsystem.com..aax-dtb-web.amazon-adsystem.com0...U......0...U.%..0...+....+.
0...g....ou..+.....i0g0-..+....0..!http://ocsp.sca1b.amazontrust.com06..+....0..
+....y....o...k.i.v.)y...99!.Vs.c.w..W}.
..M]&\%]....~..R.....ĠÓE. ....Aa..`...Fn.N
       q.<.H....!..jd ..q......_.@k.X.qr.nN.w.....w.Q.....y.Vm.7x...z..'....B.
.r....pXaC.
    Dokumente / girlstest.mi... / [Wireshark... / Wireshark ... /
```

Bild 1: Amazon Tracker im TCP-Stream

```
OCCHSBAZAFVAOOLLOAGZERMATALIACEDIAOIBBAAEHAFEAEAODIAEAAHSAGSENAKIAJEEBERAAIOAAOKAAAAAAIGABGASAMBIOSSMMUCAUIAORGBYGGGBCIADAGMBBAAIABGIAAIIGSGAAOAAKAAAAANALACSAFWADHA ACCGFGASIANYBSIDGA
      CCATOATAAngBWgC4ALOAXWAXABmADeAHMAPWAngBHACWAEWAJOAUYAPQBYGC3AGGAMOAELA908-AH6AQMA_gBFGC0AEpALEAMMALYC6gF5AMUADQA3ABXADQAHOARGAKEBIGCdgF0gLZAYWAXIBJADJAGVAMSAZMAZ4BpmDMAHFgPHAF18BohAdAAWAB
 AGIANAM-BHIC-X-MARADD, I SPKICH-DF JALINYAZ-QEI JADAL JASTAKA-BI (JOPP) I SPKICH-SEN AGARANAM-BHIC-X-MARADD, I SPKICH-DF JALINYAZ-QEI JADAL JASTAKA-BI (JOPP) I SPKICH-SEN AGARANAM-BHIC-X-MARADD, I
   KOMQAFQAVAAVABYAD4AQAAYABAADVAIYA1QBMACEAFTAL4AYQAZABZADBAIYAUYAQOBYQC3AGQUANEASA AD9AISARWAIIBOWC5GF5AMUADQA3ABGAEXQJEASCANYBQ4CBWGMAMKAZYAZ6BrAGSQCCAeOBDMAAA, T QAAAAAASQA&Q1=n-1ndex n-sha
Host: aax-eu.amazon-adsystem.com
User-Agent: Mozilla/5.0 (X1i; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
 Accept-Language: de,en-US;q=0.7,en;q=0.3
 Accept-Encoding: gzip, deflate, br
Referer: https://dl.web.de/
   Upgrade-Insecure-Requests: 1
 HTTP/1.1 302 Found
 Date: Sat, 07 May 2022 09:39:11 GMT
 Content-Length: 0
Connection: keep-alive
   Set-Cookie: ad-id=ACCBJhsar@rrk62ix@M9iM8|t; Domain=.amazon-adsvstem.com; Expires=Sun. 01-Jan-2023 09:39:11 GMT: Path=/; Secure: HttpOnlv: SameSite=None
 Cache-Control: max-age=0, no-cache, no-store, private, must-revalidate, s-maxage=0
   Expires: Thu, 01 Jan 1970 00:00:00 GMT
 p3p: policyref="https://www.amazon.com/w3c/p3p.xml", CP="PSAo PSDo OUR SAM OTR DSP COR"
    Location: https://aax-eu.amazon-adsystem.com/s/1u3?cm3ppd=1&d=dtb-pub&csif=t&qdpr=1&qdpr_consent=CPYmSEAPYmSEACnABCDECOCkAP_AAAAAAYqIapd9D7dbXFDefx_WPt00YwW0NBXC
LOCATION INTERS / ABB. 400 a. abs 260 a. abs yet en (2007 / 112 / chipple 2480 etc.) - place 127 etc.)
 KQMgAFgAVAAyABŷAD4AQAAyABôADyAIYA1gBMACeAFIĂL4AYgAZABZADBAIYAUYAPQBYĞC3AGUÄNEABSA_AD9ĂISĀRWALIBQWC5gFŚĀMUADQASAB6AEXgJÉÄSCÄNYÖQ4C8WGMAMKÀZYAZ6BrAGSgOCAeOBDMAAA.f_gAAAAASgA&dl=n-index_n-she
 Nunga-даулаулаулаулаулауларынулгандыялык Андындын Андындын Алымын Тайтардагдын Алымындагдын Алымын Алымындагдын Алымындагдын Алымындагдын Алымындагдын Алымындагдыгын Алымындагдыгын Алымы
   Permissions-Policy: interest-cohort=()
   GET /s/lu3?cm3ppd=1&d=dtb-pub&cs1f=t&qdpr=1&qdpr consent=CPYmSEAPYmSEACnABCDECOCKAP AAAAAAAYqIapd9D7dbXFDefx WPt00YwW0NBXC-
 (CCCSBAZEMAN) LAGE TAM TAILACE TAM LEAF TAM EACH TAM TAILACE TAM LEAF TAM TAILACE TAM TAILACE TAM LEAF TAM TAILACE TAM TAILACE
    AGTANWADWBHACXAH4ARQA1gBKQCDgEgALmAYQA2gB1ADQAJBASTAK4B1QDQH1KQEQACAAEgAZAA4ABBAHgARAAMABCAC-AGTANWADQBDACQAEGAKIAW4A1QB
   ACEA JOAN KAUGB TO CARILAR PARK POR TO JOAN CATAN TANG TO CATAN AND TO CATANA AND TO CATAN AND TO CATANA 
   KQMgAFgAVAAyAByAD4AQAAyABOADYAIYA1gBMACeAFIAL4AYgAZABZADBAIYAUYAQQEYgC3AGUANEASA_AD9AISARWAIIBQWC5gF5AMUADQA3ABGAEXgJEASCANYBO4C8WGMAMKAZYAZBBRADSAQCAeOBOMAAA_f
 Host: apy-ou amazon-adevetom com
 User-Agent: Mozilla/5.0 (X11; Linux x86 64; rv:78.0) Gecko/20100101 Firefox/78.0
```

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?