AP HOGESCHOOL ANTWERPEN

AP.BE

Muraena

Cybersecurity

Opleiding: Systeem en Netwerkbeheer
Academiejaar: 2025-26

Jelle Van den Broeck
Isaac Manderyck

Inhoud

Muraena

1 Voorwoord

Welkom op mijn magnum opus.

In dit werk ga ik je de beschrijving geven van de phishing tool Muraena, zo zal ik een uitleg doen over wat het is en doet, hoe het werkt maar ook zeker hoe je je hiertegen kan gaan beveiligen en hoe je kan zien dat je je aangevallen wordt.

Zo bied ik je veel leesplezier aan en hoop ik dat je er veel van bijleert.

2 Wat is Muraena

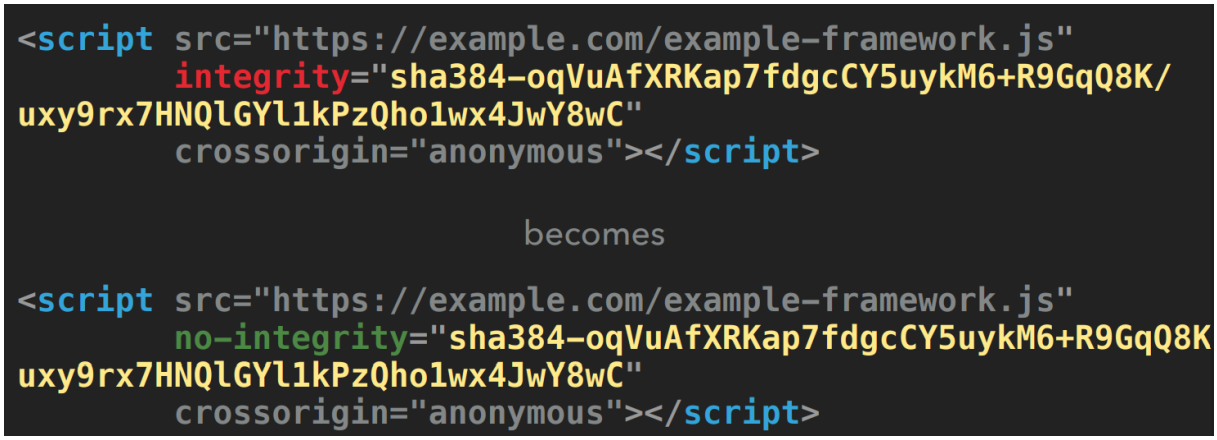
Muraena is een open source, bijna transparante reverse proxy die ontworpen is als phishing toolkit die ontwikkeld is om Man-in-the-Middle phishing-campagnes te automatiseren. Muraena gaat het verkeer realtime tussen een een slachtoffer en de officiele website onderscheppen en aanpassen, en kan zo het binnenkomende en uitgaande verkeer allemaal lezen en aanpassen zonder dat het geëncrypteerd is. Dit realiseert heel overtuigende scenario's dat het slachtoffer totaal niet door heeft dat hij/zij aangevallen word omdat je gewoon verder kan blijven surfen en op de 'echte' website zit die er toch alleszinds echt uitziet. Terwijl het slachtoffer denkt in te loggen met MFA waar deze tool voor is gemaakt krijgt de aanvaller zowel de gebruikersnaam en wachtwoord maar alsook de sessietokens van de MFA authentication.

Het doel waar deze phishing tool voor gemaakt is was om te laten zien hoe gemakkelijk het is om multi factor authentication te kunnen omzeilen als je enkel met sessietokens werkt. Uiteindelijk gebruikt deze tool geen nieuwe soort van technologie maar allemaal technologie die al lang bestaat.

Afbeelding 1: Muraena logo

2.1 Muraena vs andere phishing tools

In tegenstelling tot evilginx en andere phishing toolkits kan muraena met de hulp van necrobrowser zo goed als alles gaan automatiseren wat je bij andere tools zelf moet aanpassen als aanvaller. Ook gebruikt het een webcrawler om automatisch het web af te speuren. Zo gaat het dus javascript files gaan manipuleren zodat de computer denkt dat dit rechtstreeks van de officiële website komt en andersom.



Afbeelding 2: script omzeilen

Wat je in de afbeelding hierboven ziet is een voorbeeld van wat het onderandere allemaal kan. In dit voorbeeld veranderd het het woord integrity naar no-integrity waardoor de hash die erachter staat compleet genegeert zal worden en de browser dus geen rekening meer mee gaat houden om het script na te kijken op in dit geval phishing.

“If it works for google works for all” (Orru & Trotta, 2019, p.30)

Zoals dat ze zelf zeggen is dit ook zeker waar, omdat google heel veel verschillende factoren gebruikt die niet van éénzelfde plek komt maar van verschillende en die dan samen giet. Daarom hebben ze hun tool dus getest op Google omdat je dan weet dat het voor andere systemen dan ook gaat werken omdat Google het ingewikkeldste is.

2.2 Gevaren

Zoals elk voordeel dat deze tool kan hebben is er ook een hele grote negatieve kant aan. Het kan misschien wel gemaakt zijn door mensen met goede intenties die zichzelf ook red hat hackers noemen, om phishing campagnes te automatiseren maar aan de andere kant heb je nog altijd de mensen met slechte bedoelingen ook wel black hat hackers genoemd. Gaan zij deze tool ook kunnen misbruiken om mensen te phishen en maakt dit het hen ook veel gemakkelijker omdat dit alles automatiseert.

De gevaren hiervan zijn dat het gebruikt kan worden in grootschalige phishing attacks om grote bedrijven aan te vallen. Er kunnen zo accountovernames gebeuren of data lekken etc. ook omdat deze tool openbaar toegankelijk is als open source en gratis is wordt de drempel ook veel lager om dit te gaan gebruiken. Wat er dus tot kan leiden dat er kleinere organisaties die niet veel kennis hebben wel voor grootschalige problemen kan zorgen.

Afbeelding 3: Gevaar

3 Wat is een reverse proxy

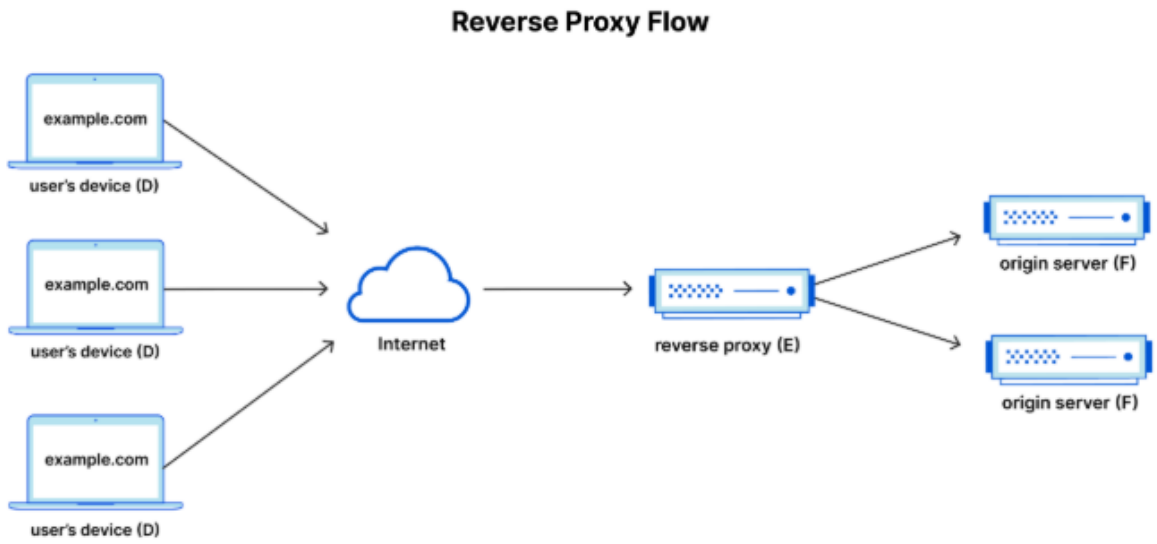
Een reverse proxy is een server die het verkeer van clients opvangt voordat die aan de werkelijke webserver geraakt. Dit wordt gedaan om de webservers te beveiligen van het internet tegen virussen. De proxy zet zich dus in als midden persoon en gaat de website bij de daadwerkelijke webserver halen, zo denkt de client dus dat de proxy de webserver is en de webserver denkt dat de proxy de client is.

Het voordeel hieraan is dat de proxy de websites kan cachen om de servers te ontlasten waardoor ze sneller kunnen werken. Ook wordt er meer aan loadbalancing gedaan en het kan de taak van versleutelen en ontsleutelen overnemen. Dit alles gaat ervoor zorgen dat alles sneller gaat werken.

Een reverse proxy biedt daarnaast ook een extra beveiligingslaag tussen het internet en de interne infrastructuur. Doordat de proxy als tussenpersoon werkt worden de IP-adressen van de echte servers dus verborgen en weet de buitenwereld niet wat de daadwerkelijke server is en waar ze staat. Daarnaast kan een reverse proxy ook doen aan webfiltering waardoor het zich dus ook kan instellen als een web application firewall om bijvoorbeeld bepaalde IP-adressen te blokkeren.

Ook kan een reverse proxy zich gaan instellen als authenticator en voor toegangsbeheer kan zorgen met een Single Sign-ON waar mensen zich op kunnen aanmelden en ze aan de hand van wie en wat ze zijn toegang krijgen tot bepaalde applicaties en hun rechten krijgen die voor hen van toepassing zijn.

Met andere woorden kan je dus heel veel doen met een reverse proxy en zijn de mogelijkheden die het allemaal kan “bijna” eindeloos.



Afbeelding 4: Reverse Proxy

4 Hoe herkennen dat je aangevallen wordt

Omdat dit werk ook bedoeld is voor de bewustwording van het gevaar van phishing aanvallen ga ik daarom ook spreken over de beveiliging en hoe je dit kan herkennen. In dit deel zal het dus gaan over het herkennen van verdachte links en website dat je mogelijk kan zien dat je wordt aangevallen voordat je je wachtwoord geeft.

Een MitM-aanval wordt steeds meer en meer geavanceerd waardoor de aanvaller bijna onzichtbaar te werk kan gaan. Maar voordat je denkt dat je helemaal niet kan zien dat je wordt aangevallen kan ik je blij maken want als je aandachtig bent kan je dit wel zien. Maar je moet wel echt heel aandachtig zijn want het verschil zit hem in de kleinste subtiele elementen.

Het grootste deel van aanvallen zoals van Muraena zullen via een mail-bericht verlopen waarbij je op een link zal moeten klikken die je dan doorverwijst naar een inlogpagina. Eerst en vooral zal je moeten nakijken naar de tekst in het bericht. Vaak staan er spelfouten in of is er een speciaal vocabulaire gebruikt omdat dit vaak komt van mensen die geen native Engels spreken. Moest dit wel allemaal kloppen kan je de zender en de link controleren. Omdat ze dit willen laten lijken dat dit bijvoorbeeld van Microsoft komt gaan ze er subtiele veranderingen in de naam steken omdat ze nooit een mailadres of website kunnen maken met exact dezelfde domeinnaam. Hier zal je dus moeten kijken naar de tekens omdat een klassiek voorbeeld is dat ze de “o” in een “0” (nul) veranderen, of ze gebruiken een koppelteken (-) in de plaats van een punt (.). Nu komt de grote “maar” want tegenwoordig worden de mensen en computers zo slim dat ze achterliggende ASCII-code zodanig kunnen aanpassen dat deze code anders is en de computer het dus anders leest maar dat de tekst die voor mensen leesbaar is er hetzelfde uitzien waardoor jij dus niet kan zien dat er iets anders staat dan bijvoorbeeld een “m”.

Als je na deze check in de mail nog niet hebt kunnen verifiëren heb je nog een kans op de inlogpagina. Eerst en vooral zal je moeten nadenken of het wel kan kloppen dat je moet inloggen want in sommige policies wordt geschreven dat je één keer om de 2 maanden maar moet inloggen en als je dat net een week ervoor gedaan hebt is het dus raar dat je opnieuw moet inloggen. Maar bijvoorbeeld ook als je online bent op je account en aan het werken bent is het ook niet normaal dat je plots een melding krijgt dat je moet aanmelden want je bent op die moment aangemeld.

5 Hoe jezelf beveiligen

Dit is denk ik wel het belangrijkste hoofdstuk van deze magnum opus. In dit deel zal ik je een uitgebreide uitleg geven hoe je jezelf hiertegen kan beveiligen ook al ken je zelf niet van IT, maar ook aan IT-organisaties die een heel bedrijf beheren. Hiervoor ga ik je stap voor stap meenemen in wat je allemaal kan doen en hoe je het moet doen.

5.1 Individueel persoon (thuis)

In dit deel van het hoofdstuk leg ik je de verschillende manieren uit waarmee je het op je thuislaptop/pc kan instellen en doen zonder dat je moet gaan betalen voor dure abonnementen op antivirussoftware.

5.1.1 Passwordmanager

Gebruik zo veel mogelijk waar het natuurlijk mogelijk is een wachtwoordmanager. Het beste is er één die je lokaal op je laptop/pc kan downloaden en niet over het internet gaat maar dat is een persoonlijke keuze. Je hebt veel betalende die online zijn en goed geëncrypteerd zijn maar die kosten “veel” geld, maar er zijn veel gratis opties die zeker evengoed zijn en lokaal worden opgeslagen. Een goede optie die ik zelf ook gebruik is “Keepass 2”, ik wil hier zeker geen reclame maken maar dat is een goede optie. Met zo een wachtwoordmanager kan je wachtwoorden opslaan met de bijhorende url zodat je de gebruikersnaam en wachtwoord automatisch kan laten invullen. Dit is een heel belangrijke hiervoor want anders heeft het niet veel nut om dit te gebruiken dat je nooit zelf je wachtwoord invult maar altijd automatisch. Want als je word aangevallen gaat de url net iets anders zijn waardoor de manager de website niet herkent en je wachtwoord dus niet ingevuld word.

5.1.2 URL’s dubbelchecken

Dit is een die je zelf elke keer aan gaat moeten denken, dat als je de link naar de website niet vertrouwd is om zelf naar de website te zoeken in plaats van via de link. Meestal is dit voor opnieuw aan te melden via Microsoft of Google en als je zelf naar de website zoek zou je dan op inlogpagina moeten komen als de mail de waarheid zegt. Maar zo weet je dus altijd zeker dat je op de echte website zit.

5.1.3 Zwakke 2FA vermijden

“2FA wat is het, wat doet het en wat drijft ze”. De grootste ergernissen op de werkvloer maar toch is het iets heel belangrijk waar we niet meer zonder kunnen in deze tijd. Maar ondanks dat het zo belangrijk is en voor veel frustraties zorgt is de manier waarop velen multi factor authentication gebruiken toch niet zo veilig en is het met tools zoals Muraena makkelijk te omzeilen.
Ja je hoort me goed, ik raad je aan om nog een extra stap toe te voegen aan je MFA. Wat ik je aanraad is om hardware authenticatie toe te voegen, je kan dit doen met je smartphone of met een externe usb. Als je je gsm gebruikt kan je met bijvoorbeeld een vinger- of gezichtscan doen en als je een usb wilt gebruiken wat de veiligste optie is kan ik je aanraden voor het gebruik van het merk Yubico. Deze usb’s zijn speciaal gemaakt voor MFA, als je wilt inloggen zal je deze moeten insteken en word er gevraagd om je eigen ingestelde pincode in te voeren en zal je daarna ook de usb moeten aanraken voordat je verdergaat. Als je dit hebt ingesteld kan er dus nooit ingelogd worden zonder die specifieke usb te gebruiken. Dus ook niet als de aanvaller er zelf zo een heeft.

Afbeelding 5: Microsoft Authenticator logo

5.1.4 Gebruik een up-to-date browser

Zorg dat je browser altijd up-to-date is door de software updates uit te voeren. Dit zorgt ervoor dat er kleine gaatjes die er in de oude software gevonden zijn gedicht worden om het de hacker steeds moeilijker te maken. Hiermee verklein je de kans om gehackt te worden omdat moderne browsers dit vaak kunnen zien en je een veiligheidswaarschuwing geven.

5.1.5 Activeer waarschuwingen bij verdachte logins

Waar bijvoorbeeld Google heel goed in is, is dat als er een vanop een onbekend systeem waar er nog nooit mee is ingelogd op jou account dat je hier een melding van ziet en dat er ook gezegd word vanuit welke locatie dit gebeurd waar jij dan op kan zeggen of jij dit bent of niet waar je de aanvaller mee kan blokkeren als het die persoon dan toch gelukt is om op jou account aan te melden.

5.2 IT-organisatie

Net zoals je eigen thuis pc is het net zo belangrijk of eigenlijk zelfs belangrijker voor IT organisaties die hele bedrijven moeten beheren dat die goed beveiligd worden omdat een hacker hier toch aanzienlijk veel schade aan kan aanrichten en dit kan een bedrijf heel veel geld kosten. Het zou niet de eerste keer zijn dat een bedrijf die gehackt word failliet zijn verklaard door data-lekken.

5.2.1 Phishing-resistente MFA verplichten

Net zoals er al uitgelegd is in het vorige deel om met hardware MFA te gaan werken kan dit al heel veel doen aan de beveiliging van je bedrijf. Als organistaie kan je dit natuurlijk gaan verplichten dat iedereen in het bedrijf dit moet gebruiken. Het enige nadeel is dat dit tijd kost om bij iedereen te gaan implementeren aan de hand van hoe groot het bedrijf is. Het instellen zelf is met één klik geregeld maar je gaat wel de tijd moeten nemen om de usb's aan te kopen en dit aan iedereen rond te delen en in te stellen.

Afbeelding 6: Yubikey

5.2.2 Security awareness campagnes

Wat er ook zeker moet gebeuren zijn security awareness campagnes. Dit zijn campagnes waarbij de IT organisaties mails rond stuurt met een verdachte link in waarmee je kan zien wie de link heeft geopend en deze personen of iedereen als het er te veel zijn een training kan geven om niet zomaar op onbetrouwbare links te klikken. Dit is maar een voorbeeldje hoe zo een campagne te werk gaat want dit gebeurd in veel verschillende maten en vormen natuurlijk. Maar het is wel heel belangrijk op regelmatig te doen want dit maakt de werknemers wel bewust van hie rap en makkelijk het gaat.

5.2.3 Cookies en session security

Dit is er eentje die rap over het hoofd gezien word maar zeker niet onbelangrijk. Wat je hiermee gaat doen is bijvoorbeeld met secure-flag ervoor zorgen dat de cookies enkel via https verstuurd worden. Of met httpOnly-flag kan je ervoor gaan zorgen dat cookies door Javascript niet meer leesbaar zijn.

Je kan er ook voor gaan zorgen dat de sessie rap vervalt zodat de token die gestolen word na een korte tijd niet meer geldig is zodat de aanvaller deze niet meer kan gebruiken. Je kan ook zorgen dat de sessies lokaal op een server worden opgeslagen in de plaats van volledig in cookies.

Afbeelding 7: cookies

5.2.4 Web filtering

Met webfiltering kan je het in en uitkomende verkeer gaan analyseren en ook gaan blokkeren als er verdachte verzoeken gedaan worden. Zo kan er moet vooraf gemaakte beleidsregels gaan gecheckt worden dat een website wel voldoet aan de eisen en als er verdachte kenmerken in worden teruggevonden kunnen deze live geweigerd worden voordat de eindgebruiker op de site terecht komt.

5.2.5 Monitoring

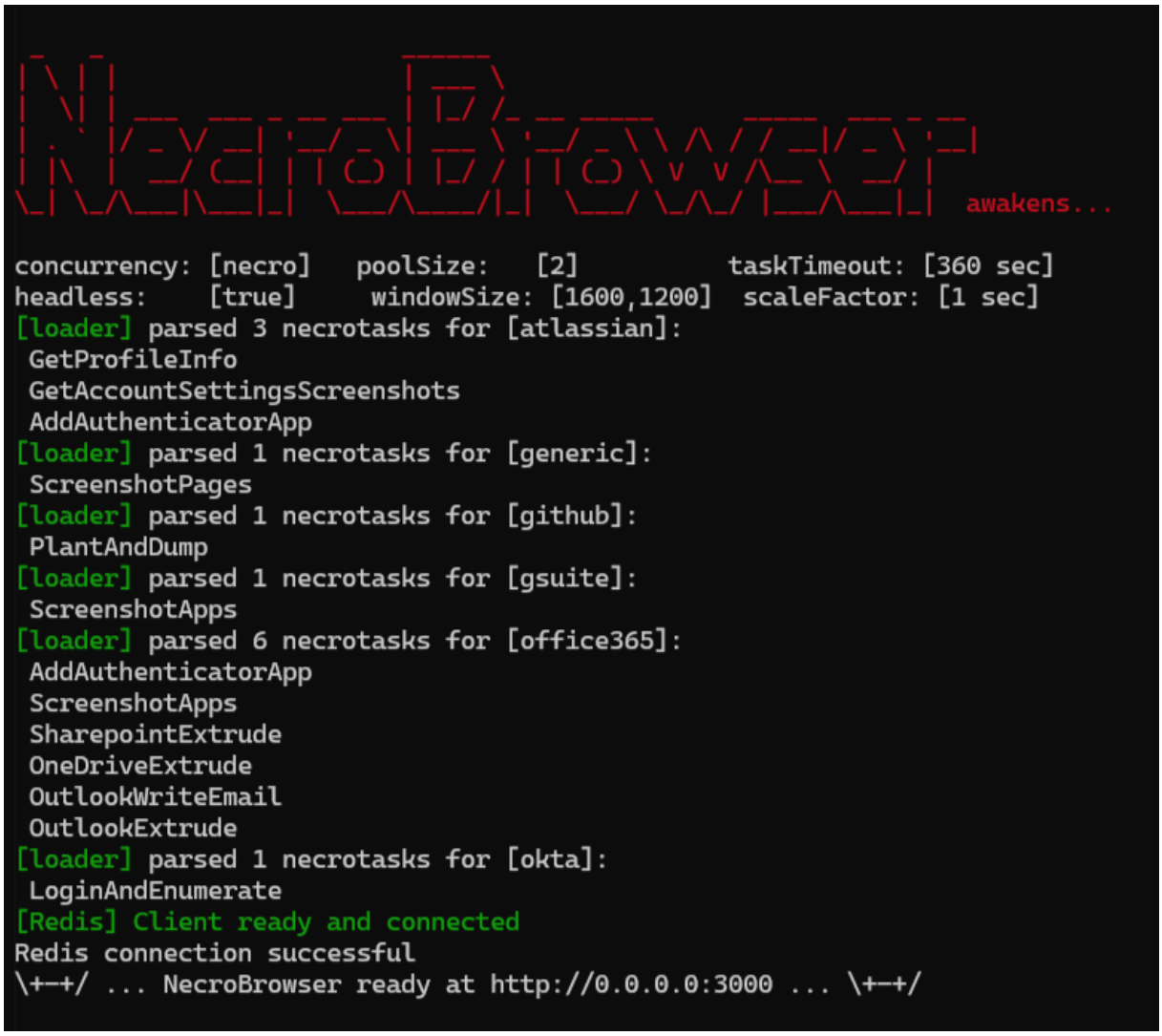
Tot slot kan ik je ook nog ten zeerste aanbevelen om aan monitoring te doen. Hier ga je zoals andere voorbeelden hierboven niet in real-time blokkeren maar kan je achteraf altijd nog zien en onderzoeken van waar de verdachte site komt. Dit kan je gaan doen door bijvoorbeeld triggers te gaan plaatsen die melding maken als er een http website bezocht is en dus niet veilig was of door een trigger te maken die een melding geeft bij alle websites die niet van het bedrijf zelf zijn of een website die nog nooit bezocht geweest is. De mogelijkheden hiermee zijn “bijna” eindeloos en dit stel je in naar je eigen wensen en doeleinden.

Afbeelding 8: Zabbix

6 Hoe werkt Muraena

Wat Muraena exact doet is dat het zich gedraagd als een reverse proxy en de echte site perfect nabootst. Zo gaat het al de gegevens van de echte site halen en stuurt die jou inloggegevens ook door naar de echte website zodat jij er als gebruiker zelf niets van merkt en de website die gebruikt word merkt het ook niet want die krijgt al jou gegevens doorgestuurd. Na het inloggen kom je ook gewoon op de echte website en kan je gewoon verder surfen zonder problemen.

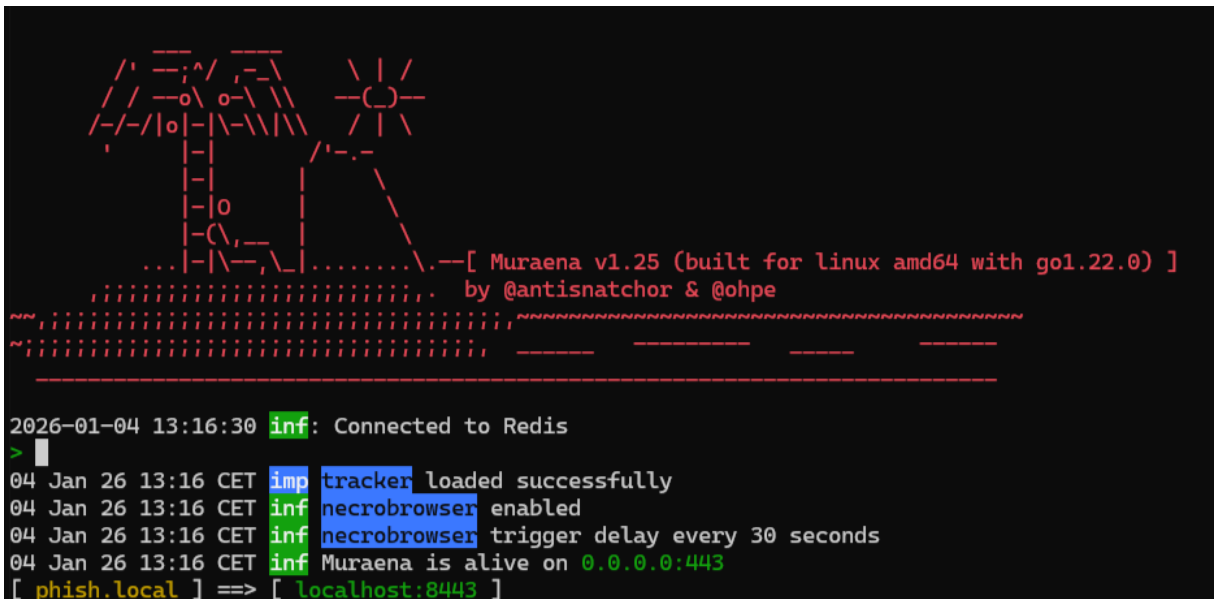
Omdat Muraena ook gebruik maakt van certificaten ziet het slachtoffer ook niets dat de site niet beveiligd is omdat het een geldig certificaat heeft. En door het gebruik van MFA kan het ook de cookies stelen om die hierna te gaan gebruiken om via Necrobrowser in te loggen met de gegevens van het slachtoffer.



Afbeelding 9: Necrobrowser startup

Ook kan je Muraena laten samenwerken met watchdog en is hiervoor ook al een sectie voorzien in de config van Muraena. Waar Necrobrowser dus zorgt voor automatisatie en sessie overname gaat watchdog meer zorgen voor de monitoring van wat er allemaal gebeurt en welke websites er bijvoorbeeld bezocht worden via de phishing link.

Zoals je zelf al wel zal doorhebben is Muraena een heel handige en interessante tool die vrij flexibel is en met veel andere tools kan samenwerken. Dit is dus de ideale tool om phishing campagnes uit te voeren omdat het eel veel automatiseert dat je het bij wijze van spreken kan starten en laten lopen en na een paar dagen pas op zou moeten terugkomen voor de resultaten. Wat dus exact is wat de mensen die dit soort campagnes uitvoeren maar dus ook black hat hackers willen.



Afbeelding 10: Muraena startup

6.1 Muraena opstellen

Vanaf je Muraena gedownload hebt van github is de structuur al redelijk klaar en vrij straight forward zo staat dus alles van configuraties in de map config en ga je enkel daar in moeten zijn. In mijn opstelling heb ik zelf gekozen om self-signed certificaten te gebruiken omdat ik geen eigen betalend domein heb en die ga je dan ook in de config moeten plaatsen met het pad waar die staan.

```
# TLS
# See: https://muraena.phishing.click/docs/tls
#
[tls]
    enable = true

    # Expand allows to replace the content of the certificate/key/root parameters to their content instead of the
    # filepath
    expand = false
    certificate = "./config/certs/_wildcard.phish.local+1.pem"
    key = "./config/certs/_wildcard.phish.local+1-key.pem"
    root = "./config/certs/rootCA.pem"
    #sslKeyLog = "./config/sslkeylog.log"

        #
        # Danger zone, be careful editing these settings
        #
        # Minimum supported TLS version: SSL3.0, TLS1.0, TLS1.1, TLS1.2, TLS1.3
        minVersion = "TLS1.2"
#    maxVersion = "TLS1.3"
#       preferServerCipherSuites = true
#       sessionTicketsDisabled =  true
        # InsecureSkipVerify controls whether muraena verifies the server's
        # certificate chain and host name.
        insecureSkipVerify = true
```

Afbeelding 11: config.toml certificaten

Omdat ik dit volledig lokaal wou doen om zo weinig mogelijk risico te hebben dat ik op een Microsoft of google account zou doen en hiervoor in de problemen zou komen omdat je wel met iets illegaal bezig bent, heb ik gekozen om de OWASP juice shop te installeren en lokaal te laten draaien maar om er wel een beveiligde verbinding mee te hebben heb ik hier ook certificaten voor gemaakt met mkcert en er een https proxy tussengezet om het zo veel mogelijk op het echte te laten lijken maar dan zonder de risico's. Hiermee kwam ik nog op een klein probleem dat Necrobrowser en de juice shop op dezelfde poort luisteren dus zet ik in het commando om de website te starten dat die luistert op poort 4000 zodat dit niet conflicteert met necrobrowser.

Om dan het werk te laten automatiseren heb ik necrobrowser ook geïnstalleerd wat ook open source is. Hiervoor moet je in de config van Muraena triggers toevoegen wanneer Necrobrowser getriggerd word en voeg je een bestand toe in de map van Muraena die instrument.necro heet. Daar zet je dan alles in wat die moet doen en met welke waardes, ik heb gekozen om een screenshot te nemen van de website en zet deze allemaal in de “extrusion” folder die je nog wel zelf moet aanmaken. Dus dan gaat Necrobrowser zelf automatisch inloggen met de gegevens die Muraena steelt van het slachtoffer die via de phishing link aanmeldt. Het handige aan deze tool is dus dat je zelf niets hoeft te doen en dat je achteraf een bewijs hebt van iedereen die via de link heeft aangemeld. Maar je kan nog veel meer doen dan enkel een screenshot nemen, iets heel nuttig maar dan vooral voor black hat hackers kan het bijvoorbeeld van Microsoft OneDrive alle documenten downloaden van het slachtoffer maar dit werkt alleen maar bij Microsoft business accounts.

```
{
  "name": "JuiceShopSession",
  "task": {
    "type": "generic",
    "name": ["ScreenshotPages"],
    "params": {
      "urls": ["https://localhost:8443/#/basket", "https://localhost:8443/profile"]
    }
  },
  "cookies": %%%COOKIES%%%,
  "credentials": %%%CREDENTIALS%%%
}
```

Afbeelding 12: instrument.necro

Afbeelding 13: link naar officiële github pagina

7 Logboek

Datum	Activiteit	Tijd
14/10/2025	Informatie inwinnen van het onderwerp en layout maken van het document	2 uur
18/10/2025	Opzoekwerk over de werking van de tool	1 uur
25/10/2025	Officiële papers lezen over phishingtoolkits	2 uur
28/10/2025	Conferentie van aankondiging hitb bekijken en papers lezen	2 uur
29/10/2025	Tekst schrijven	2 uur
30/10/2025	Opzoekwerk en schrijven	2 uur
1/11/2025	Informatie opzoeken en schrijven	4 uur
2/11/2025	Info zoeken en schrijven	2 uur
10/11/2025	Informatie opzoeken en tekst schrijven	2 uur
17/12/2025	Muraena proberen installeren	2 uur
18/12/2025	Uitzoeken hoe je muraena moet installeren	2 uur
20/12/2025	Muraena installeren en instellen	3 uur
21/12/2025	Config file instellen en uitproberen	2 uur
22/12/2025	Verder instellen en uitproberen	2 uur
23/12/2025	Troubleshooten waarom het niet volledig werkt	2 uur
24/12/2025	troubleshooten	2 uur
25/12/2025	troubleshooten	2 uur
29/12/2025	Necrobrowser installeren en instellen	2 uur
30/12/2025	troubleshooten	4 uur
2/01/2026	troubleshooten	3 uur
3/01/2026	Eigen webserver installeren en troubleshooten	4 uur
4/01/2026	Magnum opus verder schrijven	3 uur
4/01/2026	Hands-on experiment voorbereiden en maken	2 uur

8 Analyse en Conclusie

Door mijn eigen doen ben ik vaak wel het type persoon geweest dat altijd uitstelt en denkt dat hij nog tijd genoeg heeft waardoor ik na de tussentijdse evaluatie niet meer heb verder gedaan. En door een medische tegenslag die ik heb gehad eind november waar ik de eerste weken van december nog van moest recupereren heb ik me zo in tijdsnood gezet. Met als gevolg dat ik nog heel veel moest doen op het einde en ook om het praktische deel opgezet te krijgen heb ik ook heel veel tijd aan gespendeerd en verloren waardoor ik het niet volledig exact heb kunnen uitwerken maar wel over de basics ervan ben kunnen gaan.

Ik vind het zelf heel jammer dat ik niet volledig kan uitwerken en kan laten zien hoe dit in zijn werk zou gaan in het echt met zo bijvoorbeeld een nagebootste mail versturen en met een echt domein.

9 Link naar hands-on experiment video

https://ap.cloud.panopto.eu/Panopto/Pages/Viewer.aspx?id=294fa656-3162-4543-b24e-b3c800faa4e0

10 Bibliografie

ACM. (2021, November 13). *Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits*. Opgehaald van https://dl.acm.org/doi/abs/10.1145/3460120.3484765

Cons, A. H. (2022, Augustus 18). *Muraena The Unexpected Phish Michele Orru and Giuseppe Trotta*. Opgehaald van https://www.youtube.com/watch?v=EhMWS0qBP48&list=WL&index=13

HITB. (sd). *MUraena the unexpected phish*. Opgehaald van https://conference.hitb.org/hitbsecconf2019ams/materials/D2T1%20-%20Muraena%20-%20The%20Unexpected%20Phish%20-%20Michele%20Orru%20&%20Giuseppe%20Trotta.pdf

Microsoft. (2022, Juli 12). *From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud*. Opgehaald van https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

Muraena. (sd). *Muraena docs*. Opgehaald van https://muraena.phishing.click/

STRATO. (sd). *Reverse proxy – essentieel voor veiligheid*. Opgehaald van https://www.strato.nl/server/wat-is-een-reverse-proxy/

vpngids.nl. (2025, Mei 1). *Man-in-the-middle-aanval: wat is het en hoe voorkom je het?* Opgehaald van https://www.vpngids.nl/veilig-internet/cybercrime/man-in-the-middle-aanval/

11 Afbeeldingen