netidee

PROJEKTE

Fraud Seeker

Zwischenbericht | Call 17 | Projekt ID 6326

Inhalt

Einleitung

Der Betrug durch Investmentplattformen sowie durch Fake-Shops mit gefälschten Medikamenten und Nahrungsergänzungsmittel nimmt rapide zu: Gefälschte Medikamente machen bereits 10% des Pharmamarktes aus, in Nahrungsergänzungsmitteln werden teils gefährliche Stoffe gefunden und Investmentbetrug richtet in Österreich große finanzielle Schäden an.

Das Team der Watchlist Internet möchte durch Präventionsaktivitäten den Schaden reduzieren, indem vermehrt vor Betrugsseiten über Newsartikel und Warnlisten informiert wird. Dieses Ziel soll mit dem Projekt „Fraud Seeker“ erreicht werden, indem Crawler entwickelt werden, die nach betrügerischen Websites und der Werbung dafür suchen.

In der ersten Projekthälfte setzten wir uns vor allem mit den inhaltlichen Grundlagen als Basis für die technische Umsetzung auseinander. Der Schwerpunkt für die anstehende zweite Projekthälfte liegt zum einen in der Entwicklung eines Open Source Crawlers für Suchmaschinen und zum anderen in der Entwicklung eines Open Source Crawlers für die Werbebibliothek von Meta – sowie die Nutzung beider zur Evaluation dieses Ansatzes.

Status der Arbeitspakete

Arbeitspaket 1 – Projektmanagement

Im Arbeitspaket 1 „Projektmanagement“ wurde Formales zum Projektstart erfolgreich erledigt, konkret wurde (1) der Vertrag unterschrieben, (2) eine detaillierte Liste der Projektergebnisse mit Lizenz und Ort der öffentlichen Bereitstellung erstellt und abgenommen (Arbeitsblatt Projektergebnisse), (3) die Projektwebsite in Betrieb genommen und erste Blogeinträge erstellt sowie (4) die erste Förderrate beantragt. Zudem fallen in das Arbeitspaket das (5) Projektmanagement und Controlling in der weiteren Projektlaufzeit und (6) die Berichterstellung (Projektergebnisse: Zwischen- und Endbericht).

Es gibt derzeit keine Abweichungen zum Plan. Alle definierten Ziele wurden bislang erreicht.

Arbeitspaket 2 - Konzeption

Folgende Tätigkeiten wurden im Arbeitspaket 2 „Konzeption“ durchgeführt: Das Testen und die Evaluation bestehender Crawler und darauf aufbauend die inhaltliche als auch die technische Konzeption des Crawlers. Die gewonnenen Erkenntnisse wurden in einem Konzept zur Entwicklung der Crawler (Suchmaschine, Werbung) ausgearbeitet (siehe Projektergebnis 7).

Die Evaluation bestehender Crawler und Suchparamater bildete den Schwerpunkt des AP 2. Als Basis dafür diente eine Literaturrecherche, die Möglichkeiten der Clustersuche sowie der automatisierten Betrugsdetektion in den Bereichen Investment-, Medikamenten- und Nahrungsergänzungsmittelbetrug. Die Recherche zeigte, dass neben der Textphrasen-Suche noch weitere Suchparamater in Frage kommen. Dementsprechend wurde das Testen von Crawling-Möglichkeit und bestehenden Tools breit angelegt.

Textsuche über Suchmaschinen

Für die Suche nach Textphrasen wurde ein von der Watchlist Internet bereits genutztes Crawling-Tool verwendet, das darauf spezialisiert ist, Fake-Shops, Markenfälscher sowie unseriöse Dropshipping-Websites zu finden. Solche Websites verwenden häufig die immer gleichen Textbausteine, die 1:1 dupliziert und so für zahlreiche weitere Betrugs-Websites (oder auch für Werbungen auf Facebook und Instagram) verwendet werden. Die Suche nach diesen Textbausteinen ermöglicht also eine effiziente und teilautomatisierte Betrugsdetektion.

Das verwendete Tool wurde vom deutschen Unternehmen mindUp GmbH entwickelt und ermöglicht es dem Team Kategorien sowie Textphrasen anzulegen. Der Crawler überprüft anschließend die Suchmaschine regelmäßig auf neu indexierte Domains, die die angelegten Textbausteine beinhalten.

Zur Evaluation des Tools sammelte das Team der Watchlist Internet in einem ersten Schritt geeignete Textbausteine, an die sie durch Meldungen von betroffenen oder besorgten Konsument:innen kamen. In einem zweiten Schritt wurden Kategorien (Fake-Apotheken, Nahrungsergänzungsmittel und Tradingplattformen) mit den entsprechenden Textbausteinen im Crawler angelegt (siehe Abb. 1 – 3).

Abb. 1 Screenshot Kategorie „Fake-Apotheken“

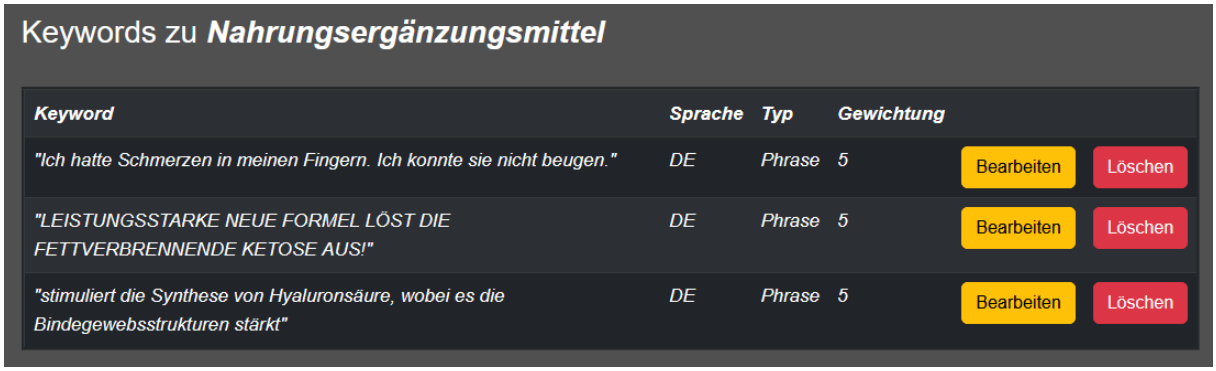


Abb. 2 Screenshot Kategorie „Nahrungsergänzungsmittel“

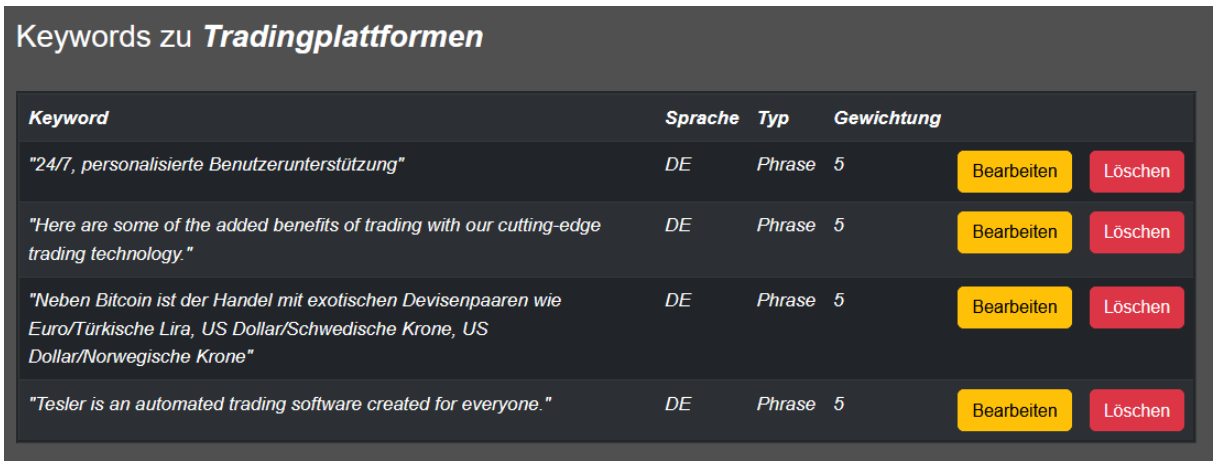


Abb. 3 Screenshot Kategorie „Tradingplattformen“

Mit dieser Vorgangsweise konnten bereits erste Ergebnisse erzielt werden, insbesondere im Bereich der Fake-Apotheken. Alle gefundenen Treffer wurden auf eigens dafür eingerichteten Warnlisten veröffentlicht (Stichtag 25.05.2023):

- 110 Fake-Apotheken
- 19 Tradingplattformen
- 8 Nahrungsergänzungsmittel

Trotz der Erfolge funktioniert die Suche nach Textphrasen nicht ohne Probleme. Bei allen drei Bereichen stoßen wir auf das Problem des sogenannten Cloakings, das zur Suchmaschine-noptimierung – auch von Kriminellen – verwendet wird. Diese verändern dabei den Quellcode gehackter Websites in einer Weise, das Bots eine andere Version der Seite sehen als menschliche Nutzer:innen. So werden Spam-Links und Weiterleitungen zu betrügerischen Websites platziert, die nur in bestimmten Umgebungen (bspw. beim Aufrufen eines Links über Suchmaschinen-ergebnisse) sichtbar sind.

Der Crawler zeigt dadurch seriöse, aber gehackte Seiten an, ein Klick auf die Crawlerergebnisse führt nicht immer zu den tatsächlichen Betrugsseiten (siehe auch Blogeintrag Von Cloaking und Crawling). In der zweiten Projekthälfte wird es u.a. darum gehen nach Lösungen dieses Problems zu suchen.

Zudem benötigt es im Bereich der Nahrungsergänzungsmittel noch weitere Recherchen, um an die jeweiligen Seiten zu kommen. Das Testen des Watchlist Internet Crawlers zeigte, dass in diesem Bereich Phrasen nicht unbedingt 1:1 übernommen, sondern von Seite zu Seite leicht angepasst werden. Sinnvoll erscheint hier nach aktuell im Trend liegenden Produkten zu suchen. Eine bereits angelaufene Kooperation der Österreichischen Agentur für Gesundheit und Ernährungssicherheit (AGES) sowie dem Bundesamt für Verbrauchergesundheit (BAVG) soll in der verbleibenden Projektlaufzeit ausgebaut werden, um diesbezüglich hilfreiche Einblicke zu erhalten.

Textsuche auf Meta-Werbebibliothek

Um Werbungen für Investmentbetrug auf Facebook und Instagram zu finden, wurde die Ad Library von Meta verwendet (https://www.facebook.com/ads/library/) und mit bestimmten Textphrasen durchsucht.

Bereits die Suche nach Textbausteinen, die in den betrügerischen Werbeanzeigen immer wieder vorkommen, stellt das Team jedoch vor Herausforderungen. Im Gegensatz zu den Websites mit den immer wieder verwendeten Textphrasen werden dem Team der Watchlist Internet nur selten die Werbeanzeigen gemeldet, durch die Betroffene auf den jeweiligen Betrug kommen. Aus diesem Grund wir dien mehrstufiges Verfahren zum Finden der Werbeanzeigen angewandt: Bestimmte Keywords wie „schnell reich werden“, „financial freedom“, „tesler“, „elon musk“ etc. werden in einem trial-and-error-Verfahren eingeschränkt. Die damit angezeigten Ergebnisse werden auf betrügerische Inhalte durchsucht und die Keywords entsprechend verfeinert, um eine bessere Suche zu erhalten.
Eine andere Vorgehensweise, um an die jeweiligen Suchphrasen zu kommen: Investmentbetrug wird oftmals über Fake-News-Artikel weiterverbreitet. Die Überschriften dieser Artikel tauchen oftmals auch in den Werbeanzeigen auf.

Aktuell (Stichtag: 26.05.2023) wird bspw. ein News-Artikel, der vorgibt von der Kronen Zeitung zu sein, mit der Überschrift „Österreicher sind sprachlos. Die gerüchte waren wahr! Die Folge darf nicht ausgestrahlt werden – der Sender ist wütend“ verbreitet.

Abb. 4 Dieser Artikel stammt nicht von der Kronen Zeitung, sondern von Betrüger:innen, die in eine Investmentfalle locken.

Die Suche nach „Österreicher sind sprachlos“ in der Meta-Werbebibliothek ergibt derzeit 19 Treffer.

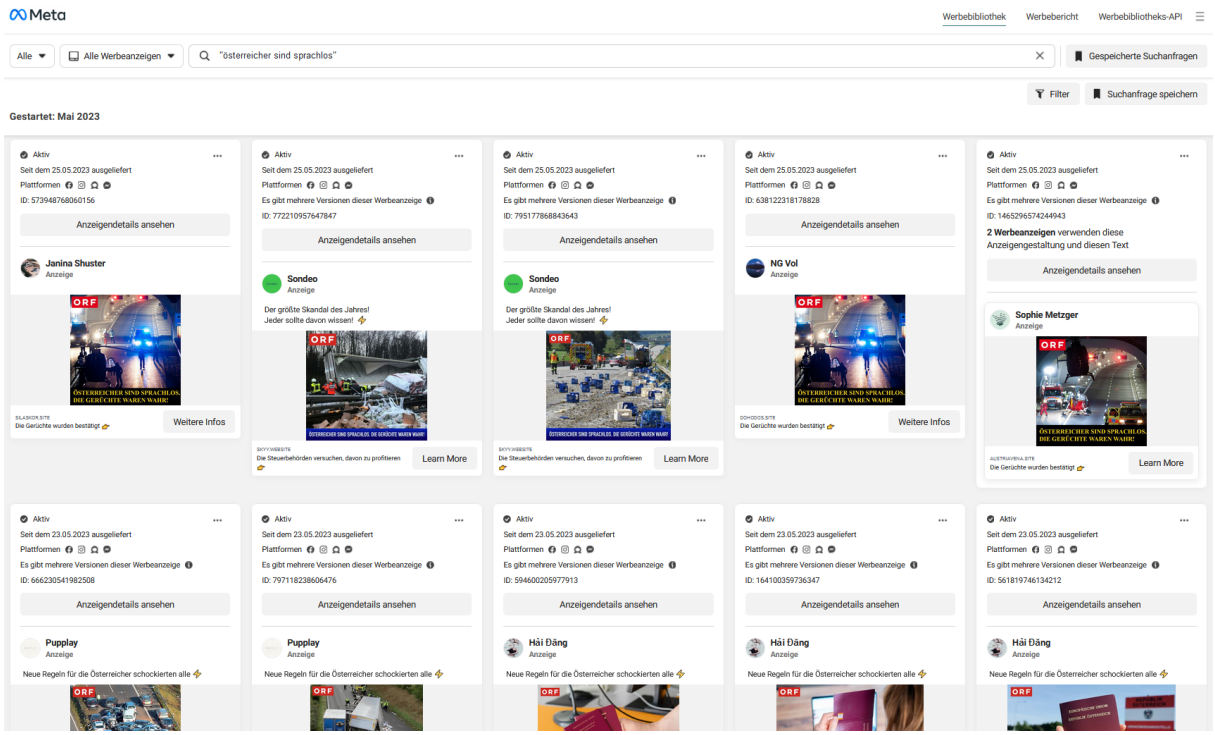


Abb. 5 Die Schlagzeile „Österreicher sind sprachlos“ taucht auch in der meta-Werbebibliothek auf

Ein weiteres Problem, dass die Clustersuche bei den Werbeanzeigen auf Facebook und Instagram erschweren kann, ist womöglich die Kurzlebigkeit der Anzeigen. Da die automatisierte Suche für die meta-Werbebibliothek noch nicht gestartet wurde, handelt es sich dabei nur um eine

Annahme. Das Team der Watchlist Internet vermutet derzeit jedoch, dass die Anzeigen nur kurz auf Meta zu sehen sind. Im weiteren Projektverlauf wird es auch darum gehen, wie damit umgegangen werden kann. Es könnte beispielsweise Sinn machen, nicht nur Phrasen zu überwachen, sondern auch die (womöglich gehackten) Facebook-Konten, um Änderungen der Werbeanzeigen mitzuverfolgen.

Weitere Suchparameter

Je nach Themenbereich können weitere Suchparameter herangezogen werden, um Betrugscluster aufzuspüren. Getestet und evaluiert wurden folgende Suchparameter:

Überwachung von Redirects: Insbesondere Domains von betrügerischen Online-Apotheken scheinen – im Gegensatz zu anderen betrügerischen Websites – erstaunlich lange erreichbar zu sein, oftmals allerdings nur über Redirects. So warnt die Watchlist Internet bspw. bereits seit 2018 vor der Website apothekerezeptfrei.com, die URL ist nach wie vor erreichbar, allerdings wird auf vetapotheke-shop.de weitergeleitet. Die Überwachung von Redirects könnte für eine langfristige Beobachtung Sinn machen, große Cluster lassen sich darüber allerdings nicht finden.

Bildersuche: Ebenfalls im Bereich des Medikamentenbetrugs zeigt sich, dass Kriminelle immer wieder die gleichen Bilder verwenden. Trotzdem scheint eine Google-Bildersuche nach diesen Bildern nicht sinnvoll, da es meistens Bilder von Einzelmedikamenten sind, die für eine gezielte Suche zu generisch sind. Sinnvoller könnte die Suche nach den Dateinamen dieser Bilder sein. Mit Hilfe des Online-Dienstes urlscan.io wurde bspw. der Dateiname „cialis-super-active.jpg“ auf mehr als 1.000 Domains gefunden. Auch die Suche nach diesem Namen in der Google-Bildersuche führt auf zahlreiche Fake-Apotheken.

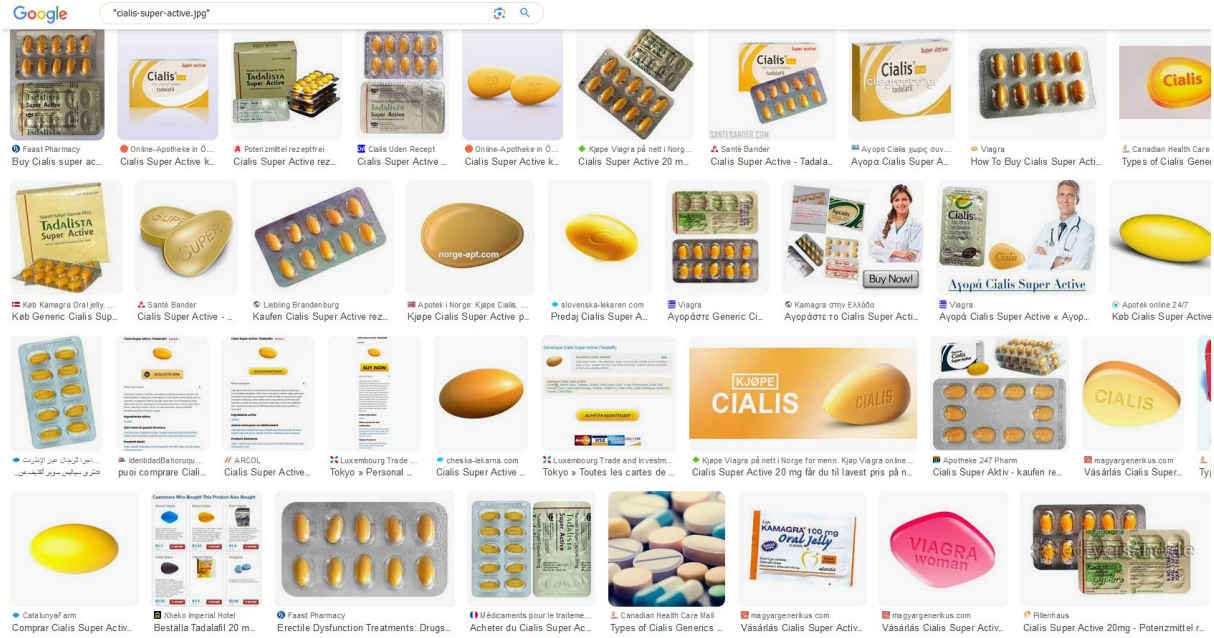


Abb. 6 Die Google-Bildersuche nach „cialis-super-active.jpg“ liefert zahlreiche betrügerische Ergebnisse

Similar Websites und Suchoperator „related“: Der Online-Dienst ulrscan.io bietet die Möglichkeit an, von einer Ausgangsdomain nach „similar Websites“ zu suchen. Die Funktion findet teilweise gar keine Treffer, selten jedoch auch sehr viele – beim Großteil der Ergebnisse handelt es sich um betrügerische Websites. Getestet wurde auch der ähnlich arbeitende Google-Suchoperator „related“, Tests mit mehreren Ausgangsdomains lieferten allerdings keine Ergebnisse.

http-Requests: urlscan.io bietet außerdem die Möglichkeit, nach auf einer Seite verwendeten Dateinamen zu suchen und so auf weitere Websites zu kommen, die diese Dateien ebenso verwendet. So stießen wir auf ein Loading-GIF („ajax-loader-table.gif“) und auf eine Javascript-Datei für ein Formular („funnel-form.js“), das auf verschiedenen betrügerischen Tradingplattformen gefunden wurde. Aufwändig ist allerdings die Suche nach funktionierenden Dateinamen.

Suche nach Knotenseiten: Nahrungsergänzungsmittel werden oftmals auf sogenannten Knotenseiten beworben, von denen aus auf verschiedene unseriöse Websites verlinkt wird (bspw. kaira.ltd.ua, wowgoods.at). Das Scrapen dieser Seiten nach Links führt so zu Betrugsclustern im Bereich Nahrungsergänzungsmittel.

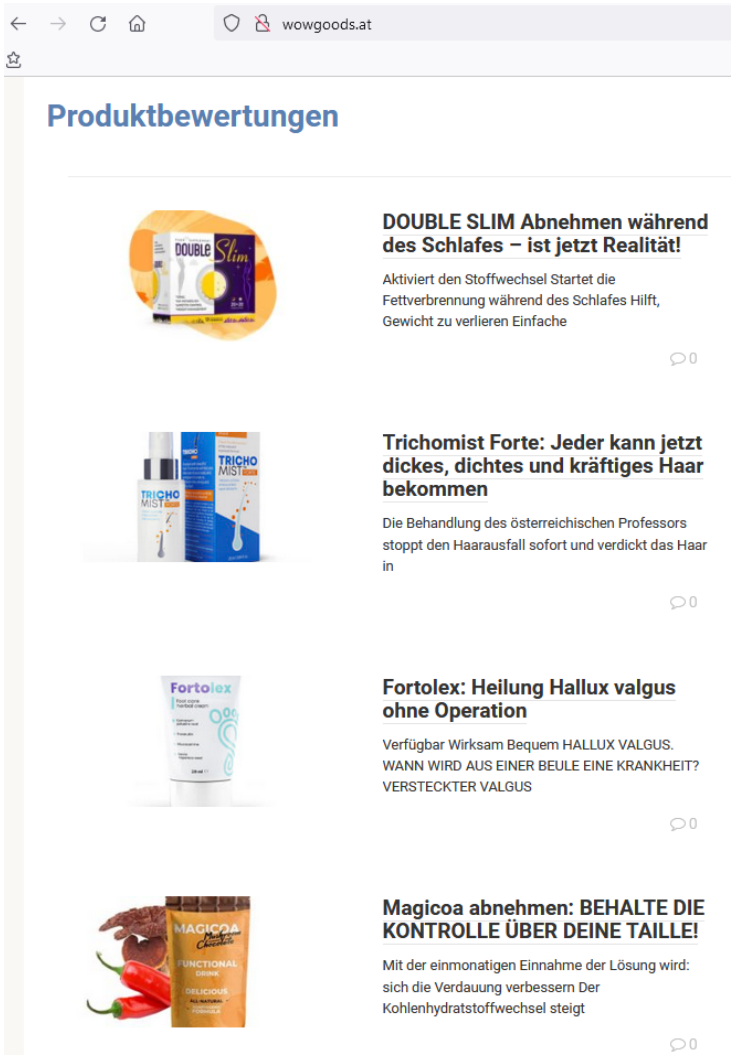


Abb. 7 Auf wowgoods.at werden zahlreiche unseriöse Nahrungsergänzungsmittel beworben.

Scamadviser Analyzer: Das Analyse-Tool des Online-Dienstes Scamadviser bietet die Möglichkeit nach Domains mit gleicher IP-Adresse, DNS, Registrar oder Hosting-Company zu suchen sowie nach Keywords und Tags (bspw. viagra, cryptocurrency etc.) zu suchen. Zwei Beispiele: Die Suche nach dem Tag „drugs – high risk“ und den keywords „viagra“, „lang=“de““ lieferte auf einem Schlag 15 relevante Ergebnisse, die Suche nach dem gleichen Registrar und nach der gleichen IP-Adresse wie pharma4health.com lieferte 18 relevante Ergebnisse.

Die Definition der Anforderungen an die Crawler in Form eines Konzeptes ist das Projektergebnis von AP2. Das Konzept fasst einerseits Sucharchitektur sowie Einblicke in mögliche Suchphrasen zusammen. Andererseits werden die technischen Anforderungen an die Crawler definiert.

Arbeitspaket 3 - Entwicklung

In Arbeitspaket 3 „Entwicklung“ geht es um (1) die Entwicklung eines Open Source Google-Crawlers, (2) die Entwicklung eines prototypischen Crawlers der Meta Ads Library, (3) die Definition des Workflows sowie (4) um die Sicherung von Whitelists für die Entwicklung. Entsprechend sind die Projektergebnisse zwei Software-Module, die nach betrügerischen Tradingplattformen und nach Fake-Shops für Medikamente und Nahrungsergänzungsmittel suchen.

Trotz existierender proprietärer Lösungen, die mit Abo-Lösungen in Anspruch genommen werden könnten und wie voran beschrieben, teilweise gute Ergebnisse liefern, wird die Entscheidung für eine Open Source Variante folgendermaßen argumentiert: Die proprietären Lösungen schaffen eine Abhängigkeit in einer asymmetrischen Situation her – zwischen der Watchlist Internet einerseits, die großes Interesse daran hat aus Qualitätssicherungsgründen genau zu den Suchmechanismen eines Crawlers zu wissen, und andererseits Unternehmen, die für die Vermarktung ihrer Tools die dahinter stehenden Suchkonzepte nicht offenlegen wollen/können. Dazu kommt, dass künftige Weiterentwicklungen nur durch eine Partei erfolgen könnten. Insofern wurde die **Entwicklung eines Open Source Crawlers** für die Suchmaschine Google in Auftrag gegeben. Genutzt wird die Google API um zu Ergebnissen zu gelangen, andere Suchmaschinen können über den objektorientierten Ansatz integriert werden.

Geplant und in Auftrag gegeben wurde auch bereits die **Web-Scraping-Lösung der Werbebibliothek-API als Open Source**. Diese technische Entwicklung birgt mehr Risiko, insofern keine anderen vorliegenden Crawler (auch proprietär) bislang dazu vorliegen. Bis September wird die erste Version vorliegen. Geplant ist die Entwicklung eines prototypischen Open-source Crawler auf Basis der Puppeteer Bibliothek für die Meta Werbebibliothek mit folgenden Funktionen:

- Google Sheets oder Textdatei zur Konfiguration der Suchwörter

- Aufruf der Meta Werbebibliothek mittels Puppeteer und Übergabe der einzelnen Suchwörter durch URL-Parameter
- Extraktion der folgenden Datenpunkte hinsichtlich der in der Abfrage zurück gegebenen Anzeigen: Suchwort, Accountname, Verifiziert: Ja/Nein, Followeranzahl des Accounts, Erstellungsdatum des Accounts, Anzahl der gefundenen Werbeanzeigen zum Suchwort, Anzahl der gesamten Werbeanzeigen des Accounts
- Ausgabe der extrahierten Daten in Google Sheets oder E-Mail

Arbeitspaket 4 – Erhebung und Qualitätssicherung

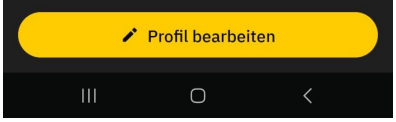
In das Arbeitspaket 4 „Erhebung und Qualitätssicherung“ fallen (1) die systematische Erhebung zu Investmentbetrug und zu (2) Betrug mit Medikamenten mit Hilfe der Crawler. Darauf aufbauend wird (3) die Qualität der Erhebungen analysiert, (4) Schlussfolgerungen für die Praxis der Watchlist Internet definiert und (5) eine Studie zu den gewonnenen Erkenntnissen verfasst.

Erste Crawling-Ergebnisse wurden bereits in AP2 zusammengefasst. Eine weitere Untersuchung, die besonders medial schon in der Projektlaufzeit auf großes Interesse gestoßen ist, betrifft die Verbreitung von Investmentbetrug via Dating-Plattformen. Insbesondere ins Visier genommen werden hier die populären Apps Tinder und Grindr, beides mobile Dating-Plattformen die in der Basisversion als kostenlose App verfügbar sind.

<u>Recherche zu Investmentbetrug via Dating-Plattformen</u>
Immer wieder gelangen Meldungen von Betroffenen bei der Watchlist Internet ein, die von perfiden Investmentbetrugs-Maschen berichten. Hierbei wurde von den Betroffenen auch öfters erwähnt, dass sie Investmenttipps von Bekannten bekommen haben. Auffällig war auch: Die Schadenssummen bei dieser Art von Betrug waren enorm hoch und: Die Zielgruppe sind hier nicht ältere Personen auf Facebook und die Scammer Piloten oder Soldaten, sondern auffällig viele Opfer sind jüngere Personen zwischen 25 und 45 Jahren. Besonders perfide ist hier: Love Scams werden verbunden mit Investmentbetrug, oft geht es um Kryptoinvestments.

Um diesem Phänomen auf den Grund zu gehen, wurde eine tiefergreifende Recherche aufgenommen. Wir haben uns mit KI-Bildern Profile auf Dating-Apps angelegt und Scammer gesucht – mit ihnen gechattet und das Vorgehen dokumentiert.

Schritt 1: Erstellung von Fake-Profilen
Mithilfe des Bildgenerierungstools „https://thispersondoesnotexist.com/“ wurden zwei Avatare erstellt, die als „Vanessa“ und „Mark“ auf unterschiedlichen Dating-Plattformen als „Bait“ (Köder) eingesetzt wurden.



Das Vanessa-Profil wurde vor allem auf der Dating-App Tinder eingesetzt. Die Persona war 32 Jahre alt, interessiert daran „neues zu lernen“ aber auch interessiert an Investments und Aktien. Das Profil wurde mit generischen Fotos von Landschaften und Essen ausgeschmückt.
Das Mark-Profil wurde hingegen auf der hauptsächlich schwulen Dating-App Grindr eingesetzt. Die Persona Mark war 33 Jahre alt und an langfristigen Beziehungen interessiert. Hier fiel die Suche nach Scammern besonders schwer, weshalb wir uns auf das Profil Vanessa konzentriert haben.

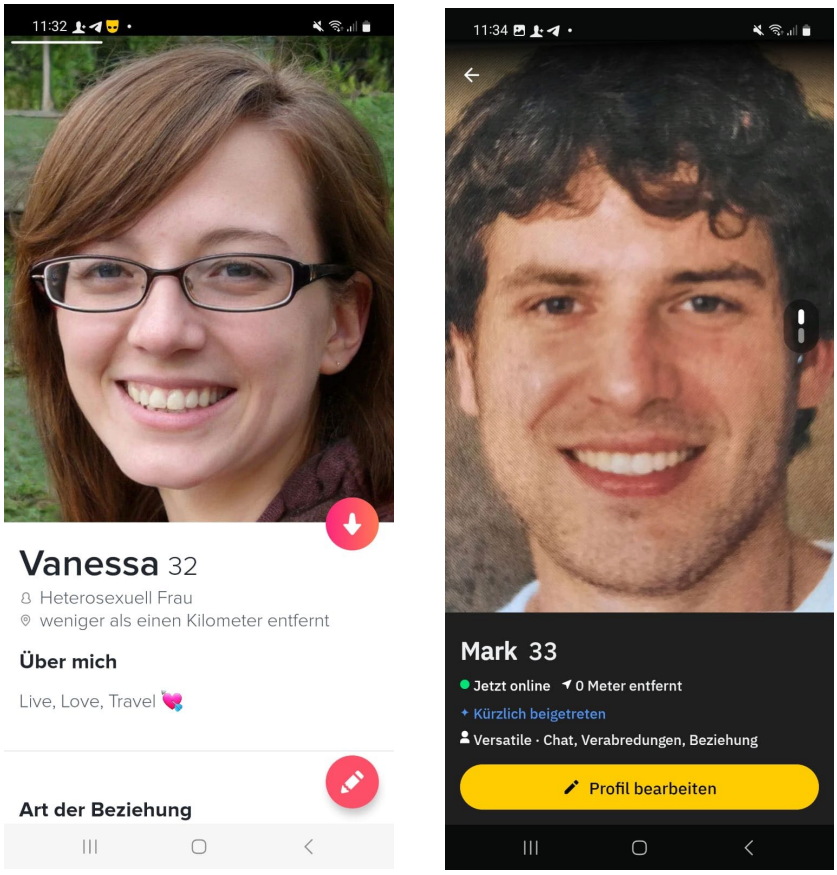


Abb. 8 Die Dating-Profile von den Personas Vanessa (Tinder) und Mark (Grindr).

Schritt 2: Suche nach Scammern
Die Dating-App Tinder wurde in der Basis-Version genutzt, die App Grindr in der Premium-Version für ein Monat abonniert, da hier sonst keine ausführliche Recherche möglich war. Auf Grindr war es uns auch wegen des persönlich-fehlenden Erfahrungshorizonts nicht möglich Profile von Scammern zu dokumentieren.

Auch auf der Dating-App Tinder hat es einige Wochen an Probieren und Herantasten an bestimmte Codes der Dating-Sprache gebraucht, um Merkmale, an denen man Fake-Profile erkennt herauszuarbeiten. Zunehmend wurde klar, dass sich Scammer für eher gutaussehende, muskulöse Profilbilder entscheiden. Die Bilder waren auch mit umgekehrter Bildersuche nicht auffindbar, was

nahelegt, dass es sich um bezahlte Inhalte (möglicherweise von Onlyfans gestohlene Daten) handelt. Die Profile waren meist spärlich ausgefüllt, keine Profilbeschreibung und wenige Interessen angegeben. Die Interessen waren immer sehr generisch: Reisen, Fitness, Aktien, Neues probieren. Möglicherweise waren sie so gestaltet, um eine möglichst breite Masse an interessierten Personen anzusprechen und nicht mit „Nischen-Interessen“ zu verschrecken.

Nach der ersten Phase, in der eruiert wurde, woran Fake-Profile zu erkennen sind, haben wir viele Stunden damit verbracht, nach genau diesen Profilen auf Tinder zu suchen. Es kamen eine Reihe an Matches zustande (Ein Match beschreibt den Prozess, wenn beide Personen das Bild des gegenüber liken. Erst dann kann ein Chat beginnen) und wir haben versucht, innerhalb kurzer Zeit ein Treffen zu vereinbaren. Waren die Personen bereit, sich mit uns persönlich zu treffen, war relativ schnell klar, dass es sich um reale Personen handelt. Diese wurden dann im nächsten Schritt einfach „Entmatched“, das Match also aufgelöst und der Chat aufgehoben.

Schritt 3: Baiting & Bestätigung
Um herauszufinden, ob wir es mit Scammern zu tun hatten wurden gezielt Themen verankert, das Thema Beruf, Geld oder einen Jobwechsel betrafen. So versuchten wir, die Scammer schneller dazu zu bringen uns Investmentplattformen zu empfehlen. Wurde dann der Köder geschluckt und Investmenttipps geteilt, haben wir vorgegeben uns nicht anmelden zu können, nicht zu wissen, wie man Kryptowährungen kauft oder vorgegeben, dass die Transaktionen nicht funktioniert haben. Die Scammer waren dazu bereit, Schritt-für-Schritt-Anleitungen zu geben, wie man Geld investieren kann und waren auch nachdem wir nicht investiert haben, noch wochenlang bereit, tägliche Konversationen zu führen. Hier wurde klar, diese Maschen zielen nicht auf schnellen Gewinn ab, sondern sind gut geplante, detaillierte Betrugsschemen, die über Monate oder manchmal Jahre durchgeführt werden.

Weiters wird dieses Arbeitspaket in der zweiten Projekthälfte umgesetzt.

Es gibt derzeit keine Abweichungen zum Plan.

Arbeitspaket 5 – Dissemination und Verwertung

Im Arbeitspaket 5 „Dissemination und Verwertung“ geht es um (1) die Überarbeitung von bestehenden und (2) die Erstellung neuer Warnlisten für die Watchlist Internet, um die (3) Erstellung von Newsartikeln zu gefundenen Bedrohungen sowie um (4) Pressearbeit – sowohl zum Projekt als auch themenspezifisch. Aktuell existieren neun themenspezifische Warnlisten auf der Watchlist Internet, um vor spezifischen Domains zu warnen. Während für betrügerische Investmentplattformen bereits eine Liste existiert (Finanzbetrug), fehlt eine spezifische Liste für Medikamenten- und Nahrungsergänzungsmittelbetrug. Da es sich dabei um Fake-Shops handelt, werden diese Domains aktuell auf die Liste betrügerischer Online-Shops.

An die Erhebung anschließend (AP 4) soll überlegt werden, ob eine neue Warnliste evtl. in Zusammenarbeit mit AGES/BAVG sinnvoll ist, um gezielter vor Medikamenten- und

Nahrungsergänzungsmittel warnen zu können. Bezüglich der Finanzbetrugs-Liste werden mögliche Überarbeitungen diskutiert werden. Warnartikel zu den gefundenen Bedrohungen werden laufen über die gesamte Projektlaufzeit erstellt.

Erste Artikel finden sich bereits auf der Watchlist Internet:

- Werbung für neue Fake-Investment-Plattform „TradeGPT“ auf Facebook, Instagram & Co.
- Bestellen Sie nicht auf cardione.at
- Vorsicht vor Abnehm-Pillen: Bestellen Sie nicht bei diaetolin.com

Zum Thema Krypto Love Scams wurde ein Vortrag (gehalten von Louise Beltzung und Julia Krickl) auf der re:publica 2023 gehalten. Der Vortrag und die Thematik fanden danach reichlich mediale Aufmerksamkeit:

- Vortrag Krypto-Love-Scams Republica
- Artikel Kryptobetrug Vice.de
- Achtung: Neue Liebes-Tricks, Kurier Titelblatt
- Krypto-Lovescam: futurezone.at

Der Vortrag bei der re:publica 2023 stellt eine Planänderung dar – die dem Vorstand der netidee zeitgerecht kommuniziert wurde – die Reise wurde genehmigt.

Zusammenfassung Planaktualisierung

Alle Anpassungen des Plan-Excels kurz zusammengefasst

Die Disseminationsaktivitäten wurden früher als geplant gestartet – vor allem ausgehend des medialen Interesses für die re:publica 2023.

Die Warnlisten konnten früher gestartet und ausgebaut werden, da schon durch den Test von existierenden Crawlern bzw. manuelle Suche genügende Funde da waren.

Öffentlichkeitsarbeit/ Vernetzung

Insbesondere im Bereich des Medikamentenbetrugs sowie der Nahrungsergänzungsmittel setzen wir auf Vernetzung. Eine Kooperation mit AGES/BVAG wurde gestartet, ein erster Austausch zum Thema Nahrungsergänzungsmittel hat bereits stattgefunden. Weitere Vernetzungstätigkeiten sind mit deutschen Stakeholdern angedacht.

Die Öffentlichkeitsarbeit fällt in Arbeitspaket 5 „Dissemination“, dort wurden erste Aktivitäten (inhaltliche Warnartikel) beschrieben. Weitere PR-Tätigkeiten werden in der zweiten Projekthälfte umgesetzt.