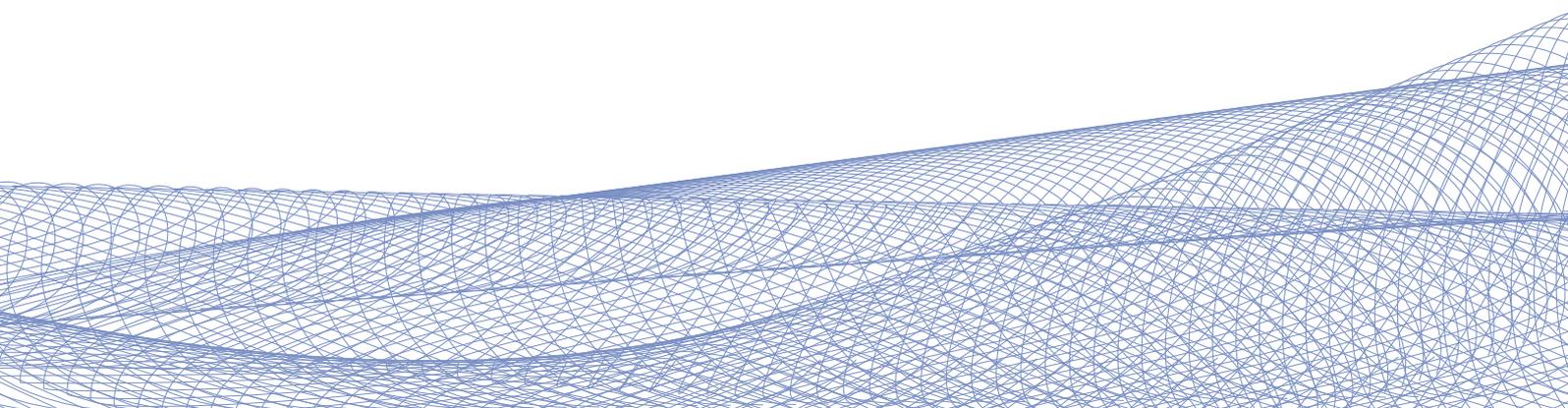


Fraud Seeker

Automatisierte Betrugsdetektion bei
Krypto-, Medikamenten- und
Nahrungsergänzungsmittelbetrug

Studienbericht
netidee Projekt Call #17

ProjectID: 6326



Inhalt

| | |
|--|-----------|
| Einleitung | |
| I | |
| Crawling Entwicklung & Methoden | 4 |
| 2 | |
| Analyseergebnisse | 8 |
| 2.1. Betrügerische Tradingplattformen | 9 |
| 2.2. Betrügerische Versand- apotheken | 15 |
| 2.3. Nahrungsergänzungsmit- tel | 24 |
| 3 | |
| Ausblick | 28 |
| 4 | |
| Quellenangaben | 29 |

Einleitung

Im Projekt „Fraud Seeker“ wurden Crawler entwickelt, um die Suche nach betrügerischen Investmentplattformen sowie nach Nahrungsergänzungs- und Medikamentenbetrug im Netz zu automatisieren.

Das Projekt wurde in enger Kooperation mit der ÖIAT-Initiative Watchlist Internet durchgeführt. Durch die in Fraud Seeker (weiter)entwickelten Crawler-Lösungen, konnten mehr Betrugsfällen gefunden werden, vor denen die Watchlist Internet über ihre Warnlisten schon in der Projektlaufzeit warnte.

Der vorliegende Studienbericht geht zuerst auf die die angewandten Methoden des Crawlings sowie auf deren Potenziale, Limitierungen und den jeweiligen Herausforderungen ein, bevor die Analyseergebnisse dargestellt werden. Nacheinander werden die Themenbereiche

- betrügerische Tradingplattformen (2.1.),
- betrügerische Versandapotheken (2.2.) und
- Nahrungsergänzungsmittel (2.3.) behandelt.

Crawling Entwicklung & Methoden

Crawlingmethoden

Was ist Crawling?

Wer täglich – wie das Team der Watchlist Internet – Websites auf Betrugsabsichten untersucht, bemerkt schnell, dass es Muster gibt: Die betrügerischen Websites sind ähnlich aufgebaut, teils ist das Layout identisch und Standardtexte (bspw. „Über uns“ oder AGB-Texte) werden Wort für Wort übernommen.

Der Grund dafür: Viele dieser Websites werden von kriminellen Netzwerken erstellt, die eine Vielzahl von Domains registrieren. Geht eine Domain offline, können Kriminelle auf Backups zurückgreifen, um die gleichen (oder ähnlichen) Inhalte auf einer anderen Domain wieder zu veröffentlichen. Darüber hinaus werden Templates betrügerischer Websites sowie die dazugehörigen Backend-Dienste (Zahlungsprozess, Kundensupport, Vertrieb etc.) an Dritte verkauft, die damit ebenfalls eine oder mehrere Websites im Namen des kriminellen Netzwerks betreiben und einen Anteil der Gewinne erhalten.¹

Das Resultat ist eine unüberschaubare Anzahl sich ähnelnder betrügerischer Domains. Mit automatisierten Detektionsmethoden kann sowohl auf den Umfang als auch auf die Kurzlebigkeit dieser Website-Cluster reagiert werden. Dafür eingesetzt werden können zum Beispiel Web-Crawler, die das Internet nach bestimmten Inhalten durchsuchen. Werden auf betrügerischen Websites z. B. wiederkehrende Code-Snippets, Text-Phrasen oder Bilder identifiziert, kann Crawling dazu genutzt werden, weitere und neu auftauchende Domains krimineller Netzwerke rasch ausfindig zu machen.

Crawling-Methoden für Clustersuche

Um geeignete Methoden zur automatisierten

(Cluster-)Suche von betrügerischen Tradingplattformen, Versandapotheken und Online-Shops für Nahrungsergänzungsmittel zu identifizieren, wurden unterschiedliche Methoden manuell getestet. Ziel war es, die Relevanz betrügerischer Merkmale zu überprüfen, aber auch die Effizienz und das Kosten-Nutzen-Verhältnis der Methoden zu bewerten.

Folgende Ansätze des Crawlings wurden getestet:

- Crawling von HTTP-Transaktionen
- Crawling von Google Analytics ID
- Überwachung von Backlinks
- Überwachung von IP-Adressen, Registrar und Hostingunternehmen
- Überwachung von Redirects
- Textbasiertes Crawling der Google-Suchmaschine
- Textbasiertes Crawling der Meta-Werbebibliothek

Crawling von HTTP-Transaktionen

Die verbreitete Nutzung von Website-Templates erklärt, warum immer wieder ähnliche Bilder, Code-Dateien oder Elemente wie GIFs auf betrügerischen Websites auftauchen. Mit Hilfe von Online-Diensten zum Scannen und Analysieren von Websites (bspw. urlscan.io) können solche Dateien bzw. die entsprechenden HTTP-Transaktionen gecrawlt werden.

Im Falle von Tradingplattformen wurden z. B. durch die Suche nach einem bestimmten Lade-GIF rund 10.000 potenzielle Scam-Websites entdeckt.² Erfahrungen, die wir – in kleinerem Maßstab – bestätigen können. Mit Hilfe von urlscan.io und der Suche nach „ajax-loader-table.gif“ fanden wir 41 Websites. Die manuelle Überprüfung ergab, dass es sich dabei ausschließlich um betrügerische Tradingplattformen handelte. Die Suche nach einem

¹ National Association of Boards of Pharmacy (2022)

² Phillips; Wilder (2020)

Formular („funnel-form.js“), das von betrügerischen Tradingplattformen für die Registrierung der Nutzer:innen verwendet wird, lieferte 47 Ergebnisse, allesamt betrügerisch.

Die Suche von HTTP-Transaktionen ist somit vielversprechend, das Problem liegt jedoch im vorab notwendigen Auffinden jener Dateien, die ausschließlich von betrügerischen Websites verwendet werden. Aufgrund dieses Aufwands erscheint eine punktuelle manuelle Suche bei Auffälligkeiten sinnvoller als ein automatisiertes Crawling von HTTP-Transaktionen.

Crawling von Google Analytics ID

Google Analytics unterstützt Website-Betreiber:innen dabei, die Performance einer Website zu überprüfen, um bspw. gut funktionierende Verlinkungen oder Keywords zu identifizieren. Auch Kriminelle nutzen das Webanalyse-Tool, um die Sichtbarkeit ihrer Websites zu erhöhen. Die Seiten erhalten dabei eine Google Analytics ID, die für die Detektion betrügerischer Websites genutzt werden kann.

Das Crawling von Google Analytics ID ist für uns vor allem in Bezug auf Nahrungsergänzungsmittel relevant. Hier sind wir auf mehrere „Knotenseiten“ gestoßen, auf denen verschiedene unseriöse Nahrungsergänzungsmittel beworben werden.

27 Seiten, die ebenfalls unseriöse Nahrungsergänzungsmittel bewerben.

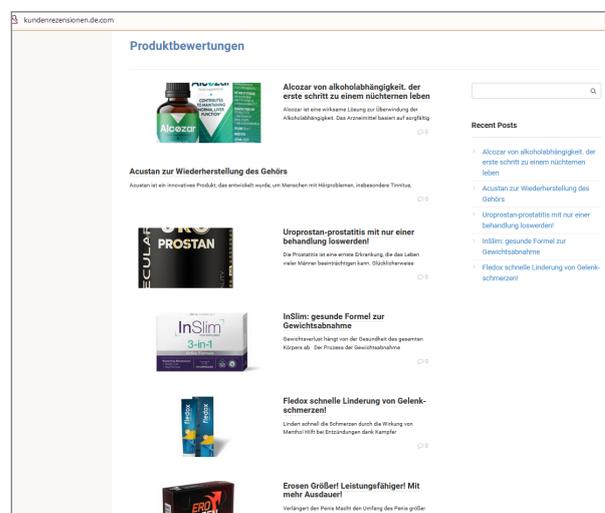


Abb. 2 Screenshot der Knotenseite kundenrezensionen.de.com.

Das klingt vielversprechend, doch auch diese Methode hat Limitierungen: So konnten verwertbare Google Analytics ID für keine Online-Shops, sondern nur für die Knotenseiten gefunden werden.

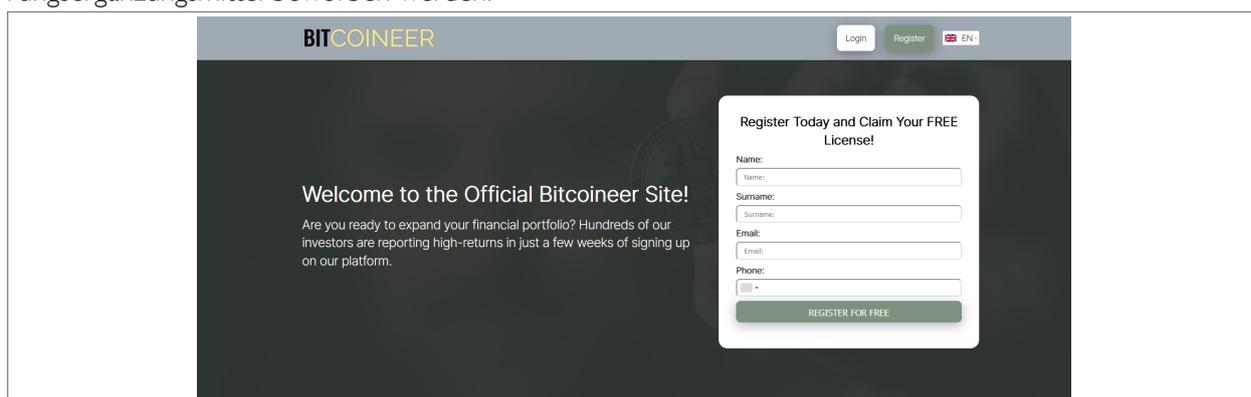


Abb. 1 Auf der betrügerischen Tradingplattform bitcoineer.io wird sowohl das Formular „funnel-form.js“ als auch das Loading-Gif „ajax-loader-table.gif“ verwendet.

Der Knotenseite kundenrezensionen.de.com ist beispielsweise die ID „ua-154900216-21“ zugeordnet. Eine Suche nach dieser ID führte zu weiteren

Die manuelle Bearbeitung solcher Seiten würde durch eine Automatisierung des Crawlings also nicht reduziert, sondern eher erhöht werden. Gleichzeitig sind nur wenige der Ergebnisse für den deutschsprachigen Raum bzw. für Österreich relevant, da unter einer Google Analytics ID oft die gleichen Produktbewerbungsseiten zu finden sind, nur in verschiedenen Sprachen.

Überwachung von Backlinks

Betrügerische Versandapotheken wickeln den Zahlungsprozess häufig über externe Seiten ab, die von den Kriminellen selbst registriert wurden. Eine einmalige Reverse-Suche nach diesen Seiten (bspw. securepaywebpage.com und paymentsafewebpage.com), lieferte insgesamt 117 Treffer. Alle Ergebnisse wurden manuell überprüft und konnten als betrügerisch eingestuft werden.

Da laufend neue Domains hinzukommen, macht ein automatisiertes Crawling zumindest für betrügerische Versandapotheken durchaus Sinn. Ein ähnliches Vorgehen für die anderen Bereiche (Tradingplattformen, Nahrungsergänzungsmittel) konnte nicht gefunden werden.

Überwachung von Redirects

Um den Traffic von alten, bereits deaktivierten Domains auf neu registrierte Domains umzuleiten, nutzen Kriminelle Redirects, also Weiterleitungen von der alten auf die neue Domain.³

Die Domain top-apotheke.com ist beispielsweise bereits seit 2019 auf der Watchlist Internet als betrügerisch gelistet. Ruft man die Seite heute auf⁴, wird man auf die ebenfalls betrügerische Seite ihremed.de weitergeleitet.

Für langfristige Beobachtungen können Redirects in diesem Bereich durchaus interessant sein; um möglichst rasch auf das Auftauchen neuer Websites

zu reagieren, ist die Methode jedoch nicht geeignet: So suchten wir mit Hilfe von Stichwörtern („apothek“ und „potenz“) nach betrügerischen Versandapotheken, die zwischen 2019 und 2020 auf der Watchlist Internet eingetragen wurden. Von den 15 gefundenen Ergebnissen waren 10 offline (ohne Redirects), 3 noch online und 2 leiteten auf eine neue Domain um. Arbeiteten die Domains mit Redirects, wurde jeweils nur eine Weiterleitung über mehrere Jahre gefunden.

Überwachung von WHOIS-Daten

Da es bereits umfangreiche Literatur zum Crawling von IP-Adressen, Domain-Registralen, Hosting-Providern und anderen WHOIS-Daten gibt, die bestätigt, dass diese Daten die Detektion betrügerischer Cluster erleichtern, wurde hier von Beginn ein automatisiertes Crawling eingesetzt.^{5,6,7} Genutzt wurde dafür das Analyzer-Tool des niederländischen Unternehmens Scamadviser, mit dem WHOIS-Daten durchsucht, erfolgreiche Suchen als Alert gespeichert und E-Mail-Benachrichtigungen eingerichtet werden können. Zwischen 22.05.2023 und 31.08.2023 lieferten drei automatisierte Abfragen nach IP-Adressen, Registralen oder Hosting-Providern, die auf Grundlage bekannter betrügerischer Domains ermittelt wurden, 112 Treffer, mehr als 90% davon waren betrügerisch.

Textbasiertes Crawling der Google Suchmaschine

Auch die Suche nach Textphrasen über die Google Suchmaschine ist nicht nur in der Literatur zu Betrugsdetektion, sondern auch in der täglichen Arbeit der Watchlist Internet bekannt. So werden Fake-Shop-Cluster von den Redakteur:innen immer wieder durch die Suche bestimmter Phrasen ausfindig gemacht.^{8,9,10}

3 Chen; Freire (2021)

4 zuletzt aufgerufen am 13.12.2023

5 National Association of Boards of Pharmacy (2022)

6 Prieto u.a. (2021)

7 Phillips; Wilder (2020)

8 Watchlist Internet (2020a)

9 Watchlist Internet (2023a)

10 Watchlist Internet (2020b)

Um dieses Vorgehen auch für betrügerische Versandapotheken, Tradingplattformen sowie Fake-Shops für Nahrungsergänzungsmittel, anwenden zu können, wurden in einem ersten Schritt Textphrasen gesucht für eine manuelle Suche. Konnten damit relevante Ergebnisse erzielt werden, wurden die entsprechenden Phrasen in einen im Forschungsprojekt entwickelten Web-Crawler eingespeist.

Der Crawler lieferte fast täglich Ergebnisse, die manuelle Bewertung der Ergebnisse war jedoch mit einem hohen Bearbeitungsaufwand bei relativ geringem Output verbunden. Der Grund dafür: Betreiber:innen betrügerischer Websites nutzen Cloaking, um automatisierte Betrugsdetektion mittels Crawler zu erschweren. Je nach Nutzer:innen-Anfrage werden dabei andere Versionen der Seite angezeigt. So landen Crawler auf für sie irrelevanten Seiten, während menschliche Nutzer:innen zu betrügerischen Seiten oder Spam-Links geführt werden. Umgehen werden kann dies, indem der Crawler bspw. durch das Zwischenschalten von VPN-Netzwerken menschliches Verhalten simuliert.¹¹

Textbasiertes Crawling der Meta-Werbebibliothek

Die Meta-Werbebibliothek liefert eine mögliche wichtige Quelle, um relevante Betrugsfälle frühzeitig zu finden. Entwickelt wurde deshalb im Rahmen des Forschungsprojekts ein Crawler, der automatisiert in der Werbebibliothek nach Begriffen sucht. Automatisiert ausgelesen wurden die folgenden Informationen: Datum, Suchbegriff, Facebook Profil/Page, Werbeanzeigen (mit dem Suchbegriff), Anzahl der vom Profil insg. geschalteten Werbeanzeigen, Verifiziert-Status, Follower, Erstellungsdatum, Profil-Link, Werbeanzeige-Link. Die Ergebnisse werden gesammelt als CSV ausgespielt.

Beim Crawling der Meta-Werbebibliothek Ad-Library erwies sich die Suche nach den richtigen Phrasen und Begriffen am schwierigsten. Es muss laufend an der Verfeinerung der Suchbegriffe gearbeitet werden, die zeitabhängig in ihrer Relevanz sind („schnell reich werden“, „elon musk“, „armin assinger“ etc.).

Das Auslesen und in Folge den gesammelten Zugriff auf diese Informationen verringert den Arbeitsaufwand in der manuellen Überprüfung von potenziellen Betrugsfällen erheblich. Dennoch ist die Überprüfung auch weiterhin mit hohem manuellen Aufwand verbunden, da die Links individuell geöffnet und überprüft werden müssen.

¹¹ Chen; Freire (2021)

Analyseergebnisse

Ergebnisse der automatisierten Suche nach betrügerischen Tradingplattformen, Versandapotheken und Nahrungsergänzungsmittel-Shops.

Betrügerische Tradingplattformen

Strukturelle Erkennungsmerkmale

Investmentangebote online boomen, ob in Gold, Krypto-Währungen oder Aktien investiert wird, versprochen werden hohe Gewinne. Auch im österreichischen Cybercrime Report 2023 wird vor betrügerischen Finanzangeboten – auch bekannt als Cyber Trading Fraud gewarnt – in diesem Bereich werden exorbitant hohe Schadenssummen gemeldet, die Dunkelziffer bei dieser Art von Betrug könnte auch höher sein als bei Fake-Shops. Zwischen seriösen und unseriösen Angeboten zu unterscheiden, ist auch für Expert:innen schwierig. Einige Merkmale können allerdings Aufschluss darüber geben, ob ein Anbieter rechtmäßig handelt, sie sind im Folgenden beschrieben.

Mit der steigenden Anzahl an betrügerischen Websites und Angeboten, diversifizieren sich auch die Erkennungsmerkmale.

Einige Merkmale, die auf den ersten Blick identifiziert werden können, geben jedoch Hinweise auf Betrug:

- Bewerbung von automatisiertem Trading
- Investment Pläne (meist 3 Stufen)
- Berühmte Persönlichkeiten als Testimonials

Investment Pläne (3-stufig)

Die betrügerische Website stablegrowthexchange.com bietet beispielsweise einen dreistufigen Investmentplan an: Einsteigen kann man mit der „Basic“ Version um 500 US \$, für das „Essential“-Paket werden schon 1.000 US \$ verlangt, das „Selective“-Paket bekommt man ab 5.000 US \$. Bietet eine Trading-Plattform ähnliche dreistufige „Pakete“ an, ist in den meisten Fällen von Betrug auszugehen.

Berühmte Testimonials

Ein weiterer Hinweis sind prominent auf der Startseite platzierte Fake-Testimonials. In dem hier angeführten Beispiel geben gleich drei der reichsten Männer weltweit eine Empfehlung für bitindexai.org ab.

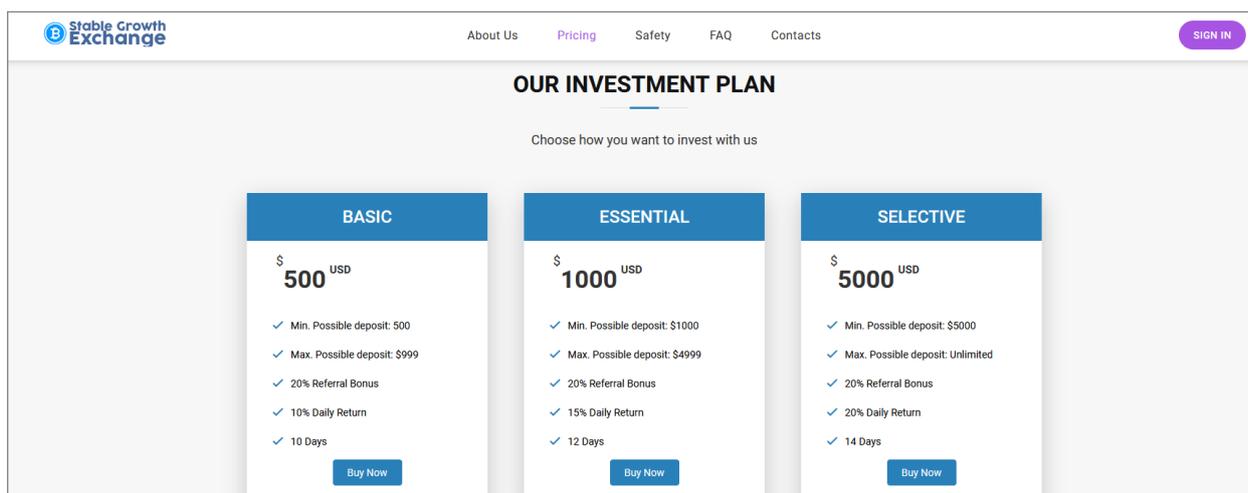


Abb. 3 Die betrügerische Website stablegrowthexchange.com bietet einen dreistufigen Investmentplan an: Einsteigen kann man mit der „Basic“ Version um 500 US \$, für das „Essential“-Paket werden schon 1.000 US \$ verlangt, das „Selective“-Paket bekommt man ab 5.000 US \$.

Finden sich solche oder ähnliche Testimonials von Persönlichkeiten wie Jeff Bezos, Bill Gates, Elon Musk oder Stars aus der Film- oder Musikbranche ist von Betrug auszugehen. Teilweise werden auch Bilder lokaler Persönlichkeiten verwendet, um solche Angebote zu bewerben, in Österreich wird bspw. vermehrt mit dem ORF-Moderator Armin Wolf geworben.

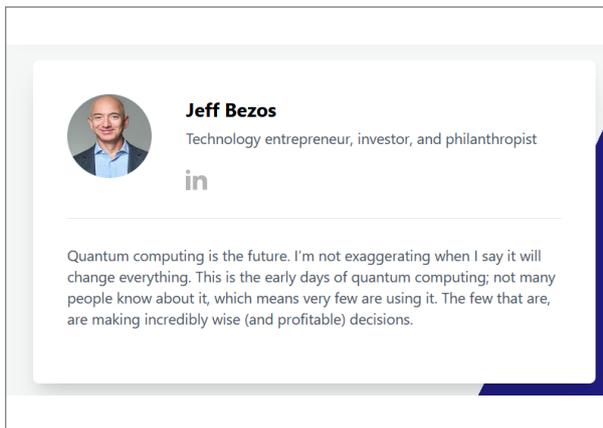


Abb. 4 <https://bitindexai.org/de/> wirbt mit Jeff Bezos, Elon Musk und Bill Gates auf seiner Startseite.

Dreistufige „Investmentpläne“ und Testimonials von berühmten Persönlichkeiten sind auf den ersten Blick ein Hinweis auf Betrug.

Abfrage der Telefonnummer

Ein Merkmal, das viele der unseriösen Trading-Plattformen vereint ist, dass diese bei der Registrierung bzw. Neuanmeldung sehr wenige Daten abfragen. Allerdings wird in fast allen Fällen nach der Telefonnummer der Interessent:innen gefragt.

In einem weiteren Schritt werden Personen, die an dem Angebot Interesse bekundet haben, per Telefon oder diverse Messenger wie Whatsapp, Signal, Facebook Messenger oder Telegram kontaktiert. Die Kontaktperson gibt sich als Investmentberater:in aus und drängt die betroffene Person zu investieren.

So wird die Abfrage der Telefonnummer auf der Startseite oder im Registrierungsformular, zu einem eindeutigen Zeichen für Betrug.

Installationsaufforderung Remote Desktop Control

Ein weiteres Indiz ist die Installation von Remote Desktop Control-Software (RDC) wie TeamViewer oder Anydesk. Wird auf einer Website auf ein solches Programm hingewiesen, kann von Betrug ausgegangen werden.

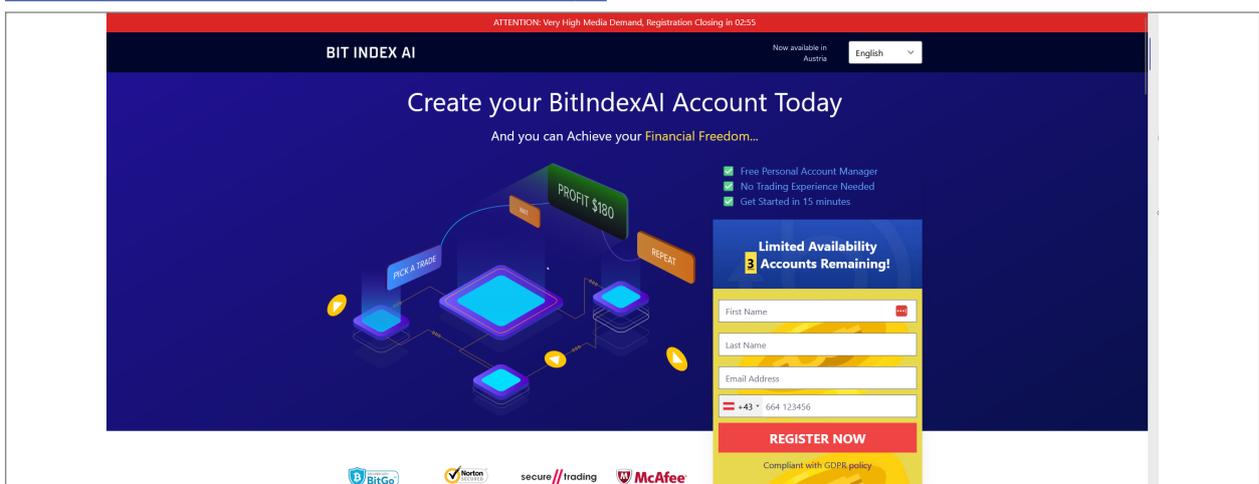


Abb. 5 <https://www.bitindexai.pro/>

Nicht alle CTF-Plattformen geben schon auf der Startseite preis, dass sie mit RDC-Lösungen arbeiten. In anderen Fällen wie ersichtlich in Abbildung 6., allerdings schon.

Das Erwähnen bzw. Bewerben von Remote Desktop Control Software ist ein klarer Hinweis auf Betrug.

Kein Impressum oder verdächtiger Unternehmenssitz

Gibt es kein Impressum, ist von einem unseriösen Anbieter auszugehen. Doch auch ein Impressum ist keine Garantie für Seriosität.

In Impessen werden besonders oft von betrügerischen Akteuren die folgenden Unternehmenssitze angegeben:

- Sitz auf „St.Vincent and the Grenadines“,
- Sitz auf „Commonwealth of Dominica“,
- Sitz auf „Marshall Islands“
- Auch angegeben werden gerne generische Ortsangaben wie „United Kingdom“ oder „Hong Kong“.

Eine Überprüfung der Adressen ist jedenfalls wichtig, denn die Suche auf Google Maps ergibt meist, dass es sich um leerstehende Gebäude oder private Wohnsitze handelt, meist ohne jegliche Verbindung zu der in Frage betreffenden Website.

Gibt es kein Impressum, oder ein generisch gehaltenes Impressum mit Sitz auf Inseln wie St.Vincent, Dominica, Marshall Islands oder Hong Kong, kann von unseriösen Anbietern ausgegangen werden.

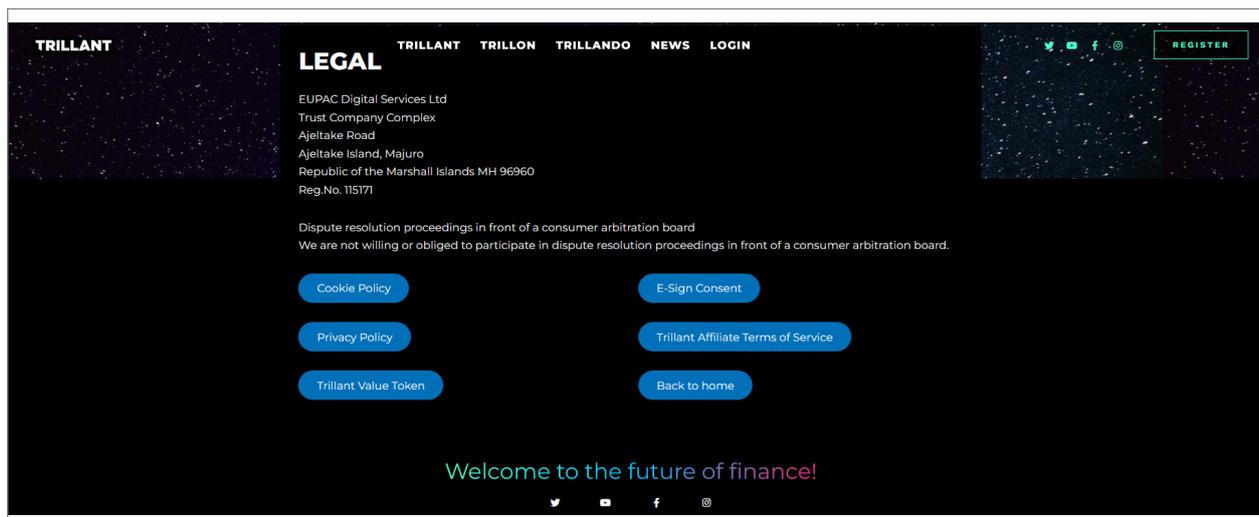


Abb. 6 <https://trillant.com>

Beispiel eines seriösen Impressums

Im Vergleich dazu, sieht das Impressum von einem registrierten Trader wie Bitpanda wie folgt aus: Es gibt vollständige Angaben zu der Adresse des Unternehmens, der Geschäftsführung, Kontakt, Handelsregister, Aufsichtsbehörde, Anwendbares Recht, Streitschlichtungsstellen und Umsatzsteuer-ID.

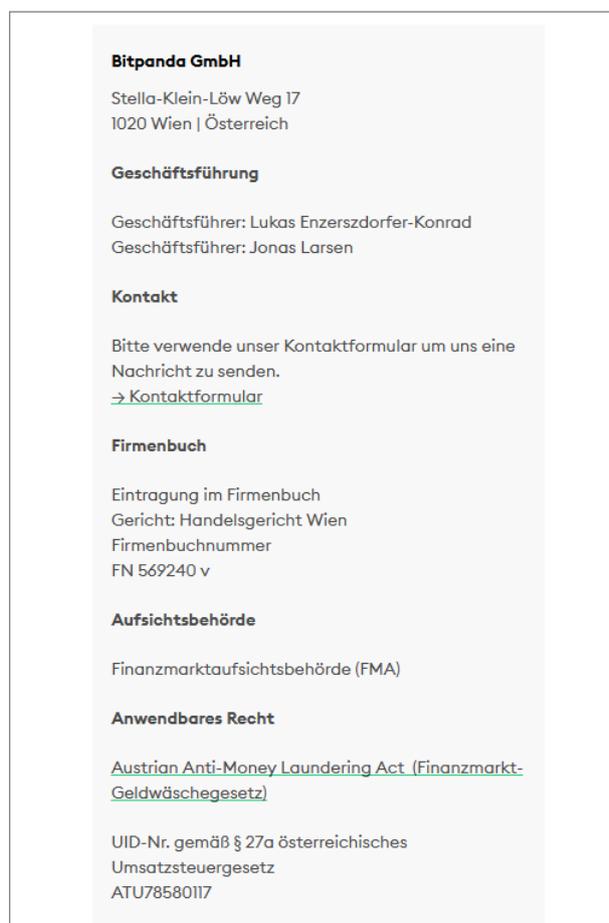


Abb. 7 Seriöses und vollständiges Impressum von bitpanda.com/de/.

Weitere strukturelle Merkmale

Um betrügerische Angebote automatisiert erkennen zu können, können folgende Erkennungsmerkmale formalisiert werden:

- Existiert https
- Wird verhindert, dass die Seite von der Suchmaschine indexiert werden kann

- Sprache: Ein seriöser Anbieter mit Zielmarkt D A CH wird automatisiert deutsch kommunizieren
- Onepager-Websites
- Bewertungen bei Trustpilot
- unrealistische Gewinnversprechen
- Positive Textmuster: Erwähnung von Streitschlichtungsstelle oder Aufsichtsbehörde
- Negative Textmuster: Remote Desktop Control, Namen von Prominenten
- Betrügerische Seiten haben häufig keine sitemap.xml – das ist für größere Firmen, die etwas verkaufen wollen, Standard, für One-Pager und Websites, die nur kurz bestehen unnötig.

Regulierung der Bewerbung von Finanzdienstleistungen

Meta hat gesonderte Werberichtlinien für die Bewerbung von Finanzprodukten auf seinen Plattformen erlassen. Laut Meta darf auf Facebook und Instagram nicht für Finanzprodukte und -dienstleistungen geworben werden, die mit irreführenden oder betrügerischen Verkaufsförderungsmethoden in Verbindung gebracht werden.

Folgende Produkte dürfen laut Meta nicht beworben werden:¹²

- Kurzzeitkredite
- Gehaltsvorschüsse
- Kautionen
- Kurzfristige Kredite mit einer Laufzeit von maximal 90 Tagen
- Pennyauktionen, kostenpflichtige Gebotsauktionen oder ähnliche Geschäftsmodelle
- Binäre Optionen
- Initial Coin Offerings (ICO)
- Handel mit Differenzkontrakten
- Irreführende Dienstleistungen zur Konsolidierung, zum Erlass oder zur Refinanzierung von Studentendarlehen

Zudem bestehen folgende Einschränkungen bei der erlaubten Bewerbung von Finanzprodukten:

¹² <https://transparency.fb.com/de-de/policies/ad-standards/deceptive-content/prohibited-financial-products-and-services/>, zuletzt aufgerufen 22.12.2023

„Werbtreibende dürfen Anzeigen schalten, die für Kreditkarten, Kredite oder Versicherungsdienstleistungen werben, sofern sich die Anzeigen nur an Personen ab 18 Jahren richten und auf der Zielseite der Anzeige (Landingpage) keine personenbezogenen Informationen abgefragt werden.

Werbtreibende müssen ggf. in den gewünschten Zielländern, auf die sie ihre Werbung ausrichten, über die erforderlichen Zulassungen verfügen, um Werbung für Finanz- und Versicherungsprodukte und -dienstleistungen schalten zu können. Meta kontrolliert möglicherweise, ob alle erforderlichen Genehmigungen eingeholt wurden bzw. ob die Werbtreibenden autorisiert sind, solche Werbung zu schalten. Die Werbtreibenden sind dazu verpflichtet, alle geltenden Gesetze und Vorschriften einzuhalten, einschließlich sämtlicher Genehmigungsaufgaben und Offenlegungspflichten.“

Auch hinsichtlich der Bewerbung von Kryptowährungen bestehen folgende Einschränkungen:

„In Werbeanzeigen dürfen ohne vorherige schriftliche Genehmigung keine Handelsplattformen und Software für Kryptowährungen sowie zugehörige Dienstleistungen und Produkte beworben werden, welche die Monetarisierung und den Weiterverkauf von, den Eintausch gegen oder das Spekulieren auf Kryptowährungen ermöglichen.“¹³

Trotz dieser Regelungen werden der Watchlist Internet viele betrügerische Werbeanzeigen gemeldet, die weitreichend auf Meta-Diensten verbreitet werden. Darunter fallen vor allem Fake-News Artikel, die sich der Namen von Persönlichkeiten des öffentlichen Lebens, bzw. Fernseh-Persönlichkeiten bedienen (Armin Assinger, Barbara Karlich, Christoph Grissemann, Miriam Weichselbraun, Armin Wolf, etc.) und betrügerische Finanzprodukte bewerben. Meist verlinken diese Fake-Artikel auf einfache Kontaktformulare, in denen die Betroffenen ihre Daten (Name, Telefonnummer, E-Mail-Adresse) eingeben und dann von den Kriminellen kontaktiert werden.



Abb. 8 Werbeanzeigen für Fake-Newsartikel, die Armin Wolfs Namen zur Bewerbung von Finanzbetrug missbrauchen.

Diese Fake-News Artikel erfüllen den Bestand der Abfrage persönlicher Informationen, der in der oben zitierten Richtlinie geregelt ist, dennoch werden diese Werbeanzeigen weiterhin auf Meta genehmigt und an tausende Betroffene ausgeliefert.

Hierbei bedienen sich die Kriminellen einer Lücke in den Richtlinien, laut Meta dürfen nämlich folgende Arten von Anzeigen von Werbtreibenden auch ohne Autorisierung bzw. ohne Einschränkungen geschaltet werden:

- z. B. Markenwerbung für Banken oder Versicherungsgesellschaften
- Anzeigen für Nachrichtenartikel, vorausgesetzt, sie enthalten keine Angebote für Kreditkarten, Kredite oder Versicherungsdienstleistungen

Da die Anzeigen für Nachrichtenartikel ausgenommen sind und Meta nicht alle Inhalte von beworbenen Nachrichtenartikeln überprüft, stellen diese das optimale Schlupfloch für die Bewerbung von Fake-News dar.

¹³ https://transparency.fb.com/policies/ad-standards/?source=https%3A%2F%2Fwww.facebook.com%2Fpolicies_center%2Fads%2Fprohibited_content%2Fmisleading_or_false_content, zuletzt aufgerufen 22.12.2023

Qualitative Ergebnisse

Wie im vorherigen Abschnitt erwähnt, wurden der Watchlist Internet vor allem Fake-News Artikel gemeldet mithilfe derer betrügerische Finanzprodukte beworben wurden. Allein die manuelle Suche nach dem Namen „Armin Assinger“ im Dezember 2023 ergibt über 1.100 Suchergebnisse in der Meta-Werbebibliothek. Die meisten dieser Werbeanzeigen bewerben Fake-News Artikel, die vorgeben von OE24, Kronen Zeitung, Heute oder ORF zu sein und über „Clickbait“-Skandal-Headlines versuchen die Aufmerksamkeit von Usern zu erhaschen.

Die automatisierte Suche nach betrügerischen Finanz- bzw. Tradingplattformen erwies sich allerdings als deutlich schwieriger. Mithilfe des Suchmaschinen-Crawlers konnten nur 46 Plattformen gefunden werden, im Zeitraum zwischen 01.04.2023 und 30.09.2023. Die Suchphrase, die zu den meisten Ergebnissen (10 Plattformen) geführt hat, war folgende, „Tesler is an automated trading software created for everyone.“

Die geringe Anzahl der Funde, könnte unterschiedliche Gründe haben, u. a.:

- (A) Viele Botschaften auf unseriösen bzw. betrügerischen Tradingplattformen werden in Bild oder Videoformat präsentiert. Hierdurch wird die Effektivität von Textsuchen ausgehebelt.
- (B) Über Cloaking könnten die Ergebnisse verfälscht bzw. nicht auffindbar werden (siehe Kapitel I).
- (C) Ein Großteil der Finanzbetrugswebsites besteht lediglich aus einer Landingpage mit einem Formular zur Eingabe von persönlichen Daten. Der tatsächliche Betrug passiert nachdem die Kriminellen Kontakt zu den Opfern aufgenommen haben, via WhatsApp, Telegram oder per Telefon. Erst dann werden die Betroffenen auf Fake-Tradingseiten weitergeleitet. Diese haben wenig durchsuchbaren Inhalt und enthalten oftmals nur einen Login-Bereich, einen animierten Chart zu fiktiven Aktien oder Krypto-Kursen und eine Bezahlmaske, in der Kreditkartendaten, Krypto-Wallet-Keys oder andere Zahlungsdaten eingegeben werden können. Das bietet wenig Potenzial für eine Auffindbarkeit über Suchmaschinen-Crawler.

Da auch eine hohe Fluktuation an betrügerischen Anzeigen auf Meta besteht, wurde der Einsatz des Werbecrawlers bei dieser Art der Werbung für Tradingplattformen als nicht zielführend eingeschätzt.

Betrügerische Versandapotheken

Problemlage

Bereits jede zweite Person hat Gesundheitsprodukte und nicht-rezeptpflichtige Medikamente im Internet eingekauft. 30% kaufen diese Produkte sogar bevorzugt online ein.¹⁴ Das Angebot ist entsprechend groß: Aktuell gibt es in Österreich mehr als 300 registrierte Versandapotheken.¹⁵

Neben den legitimen Online-Apotheken gibt es allerdings eine weitaus größere Zahl an betrügerischen Apotheken, deren Betreiber:innen sich auf den Kauf verschreibungspflichtiger Medikamente spezialisieren. Im Jahr 2016 schätzten Expert:innen die Marktgröße von Apotheken, die verschreibungspflichtige Arzneimittel online vertreiben auf weltweit 30.000 bis 35.000 Seiten, 92% davon werden mit krimineller Absicht betrieben, Gesetze werden dabei ignoriert. Ein Problem, das auch für den deutschsprachigen Raum relevant ist, denn rund 13% der Websites sind entweder ausschließlich deutschsprachig gestaltet oder die Sprache wurde auf Deutsch geändert, wenn sich die Nutzerin in einem deutschsprachigen Land befindet.¹⁶

Betrügerische Versandapotheken zeichnen sich dadurch aus, dass sie (1) verschreibungspflichtige Medikamente ohne Rezept anbieten, (2) gefälschte, nicht zugelassene oder nicht regulierte Medikamente verkaufen und/oder (3) keine Apothekenlizenz besitzen.

Diese drei Kriterien beruhen auf den rechtlichen Definitionen zu gefälschten und illegalen Arzneimitteln sowie den Bestimmungen zum Versandhandel mit Arzneimitteln.

Gefälschte und illegale Arzneimittel

Illegale Medikamente werden abseits der rechtlichen

Rahmenbedingungen hergestellt und/oder vertrieben. Das muss nicht unbedingt mit der Fälschung von Arzneimitteln einhergehen. So können auch originale Medikamente, die in Österreich nicht zugelassen bzw. verboten sind durch betrügerische Versandapotheken nach Österreich vertrieben werden.¹⁷

Gefälschte Arzneimittel sind eine Form von illegalen Medikamenten, die im Arzneimittelgesetz (AMG) unter § 1 Abs. 25 als Arzneimittel definiert sind, bei denen nicht nur (1) das Mittel selbst (falsche Zusammensetzung jeglicher Bestandteile, inklusive Hilfsstoffe), sondern auch (2) die Verpackung und Kennzeichnung (bspw. um abgelaufene Originalprodukte in eine Verpackung mit neuem Ablaufdatum umzupacken), (3) die Herkunft (Hersteller:innen, Herstellungs- oder Herkunftsland, Registrierungs-inhaber etc.) sowie (4) die entsprechenden Dokumente bezüglich der Herstellung oder der Vertriebswege gefälscht oder manipuliert wurden (bspw. wenn ein Medikament als österreichische Erzeugung vermarktet, aber tatsächlich in Indien hergestellt wurde).¹⁸

In der Praxis stimmt beim Großteil der gefälschten Arzneimittel das Verhältnis der Wirkstoffe nicht – das kann sowohl zu einer Unter- als auch zu einer potenziell lebensbedrohlichen Überdosierung von bestimmten Wirkstoffen führen. Unterdosierung bzw. fehlende Wirkstoffe können ebenfalls schwerwiegende Folgen haben, wie bspw. zu schwach dosierte Antibiotika, die langfristig die Antibiotika-Resistenz erhöhen oder unbehandelte Krankheiten, die diese verschlimmern oder chronifizieren können.¹⁹ Gleichzeitig sind auch zahlreiche Fälle bekannt, in denen gefälschte Medikamente nicht deklarierte Wirkstoffe enthalten.²⁰ Illegale Medikamente

14 IGEPHA - The Austrian Self Care Association (2023)

15 <https://www.basg.gv.at/konsumentinnen/arzneimittel-im-internet/versandapotheken>, zuletzt aufgerufen 21.12.2023

16 LegitScript (2016)

17 <https://www.basg.gv.at/konsumentinnen/illegaler-markt/faelschungen>, zuletzt aufgerufen 21.12.2023

18 RIS (2023)

19 <https://www.basg.gv.at/konsumentinnen/illegaler-markt/faelschungen>, zuletzt aufgerufen 21.12.2023

20 OECD; European Union Intellectual Property Office (2020)

verursachen also nicht nur einen erheblichen finanziellen Schaden für die Pharmaindustrie, sondern gefährden auch die öffentliche Gesundheit.

Versandhandel von Arzneimittel

Im Arzneimittelgesetz (Fernabsatz-Verordnung) sind die Rahmenbedingungen für den Versandhandel von Arzneimittel geregelt. Demnach dürfen nur registrierte Online-Apotheken mit Sitz in Österreich oder dem Europäischen Wirtschaftsraum Medikamente online verkaufen.²¹ Um für den Versandhandel von Arzneimittel berechtigt zu sein, gelten strenge Regeln, die in Österreich vom Bundesamt für Sicherheit im Gesundheitswesen (BASG) überprüft werden.²² Legale Versandapotheken dürfen in Österreich – anders als in anderen europäischen Länder – keine rezeptpflichtigen Medikamente online verkauft werden.²³

Außerdem wurde mit der Umsetzung der sogenannten Fälschungsrichtlinie im Jahr 2015 ein europaweites Sicherheitslogo für legale Internetapotheken eingeführt. Nur Websites, die ein solches Logo sichtbar platzieren und bei denen man mit einem Klick auf das Logo zu einem Verweis zur Legalität der jeweiligen Apotheke auf der Seite der nationalen Arzneimittelbehörde gelangt, dürfen legal nichtrezeptfreie Medikamente verkaufen.²⁴

Relevanz betrügerischer Versandapotheken

Wie aus einem OECD-Bericht hervorgeht, belief sich der Wert des weltweiten Handels mit gefälschten Arzneimitteln 2016 auf bis zu 4,4 Milliarden US-Dollar – Geld, das der Pharmaindustrie abgezweigt wird. Zu den am meisten gefälschten Medikamenten zählen Antibiotika, gefolgt von Medikamenten zur Potenzsteigerung und Schmerzmittel.²⁵

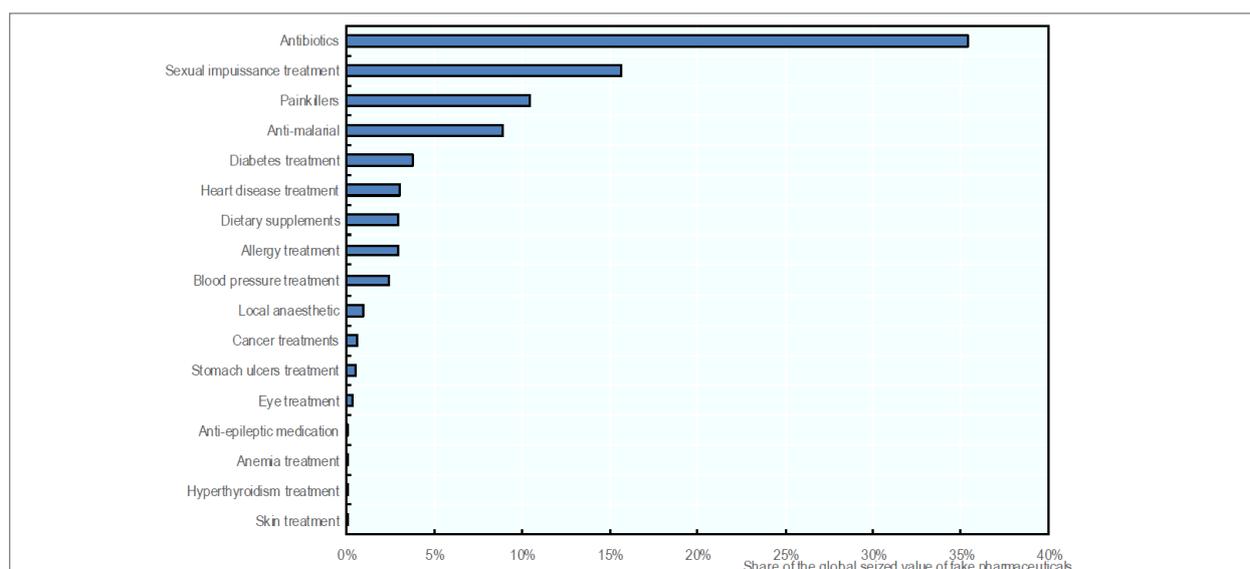


Abb. 9 Die am häufigsten vom Zoll beschlagnahmten Arzneimittelfälschungen, 2014 - 2016.

21 RIS (2023)

22 <https://www.basg.gv.at/konsumentinnen/arszneimittel-im-internet/versandapotheken/faqs-versandapotheken>, zuletzt aufgerufen 21.12.2023

23 RIS (2023)

24 BASG (2023)

25 OECD; European Union Intellectual Property Office (2020)

Der digitale Vertrieb spielt dabei eine zentrale Rolle, da unseriöse Händler:innen so die Möglichkeit haben, anonym zu agieren und gleichzeitig die Darstellung der Produkte ohne weiteres verfälschen können. Der österreichische Produktpirateriebericht 2021 benennt die Entwicklungen rund um Medikamentenfälschungen als besorgniserregend und identifiziert Online-Portale als zentralen Vertriebsweg. So wurden 2021 bei 7.983 Aufgriffen (+133% gegenüber 2020) mehr als 2,6 Millionen illegale Medikamente (+650% gegenüber 2020) beschlagnahmt. Bereits seit Jahren stellt der österreichische Zoll einen Anstieg dieser Zahlen fest, zu beobachten ist allerdings eine zusätzliche Steigerung durch den Online-Shopping-Boom während und nach der Covid-19 Pandemie, zudem wurden vermeintlich Covid-19-spezifische Medikamente wie das Wurmmittel Ivermectim von der Zollverwaltung vermehrt aufgegriffen.²⁶

Quantitative Ergebnisse

Mit Hilfe von textbasierten Crawling-Methoden sowie der automatisierten Überwachung von WHOIS-Daten konnten im Analysezeitraum (01.04.2023 bis 30.09.2023) insgesamt 443 betrügerische Online-Apotheken identifiziert werden.

Der Web-Crawler lieferte mit über 400 betrügerischen Domains einerseits die meisten Treffer, andererseits verursachte die große Anzahl der vom Crawler gefundenen Domains auch den größten Arbeitsaufwand bei der manuellen Qualitätssicherung und Bewertung der Seiten: Nur etwa 30% der vom Web-Crawler gesammelten Domains waren betrügerisch. Bei den restlichen 70% handelte es sich um eigentlich seriöse Seiten, die von Cloaking betroffen waren oder um Websites, die nicht mehr erreichbar waren. Diese schlechte Trefferquote, zeigt die Notwendigkeit, den Crawler hinsichtlich der Simulation menschlichen Verhaltens weiterzuentwickeln.

Je nach Textphrase variierte die Trefferquote sehr, entsprechend müssen die Ergebnisse jedenfalls

regelmäßig evaluiert werden, damit es zu keinen Fehlern kommt.

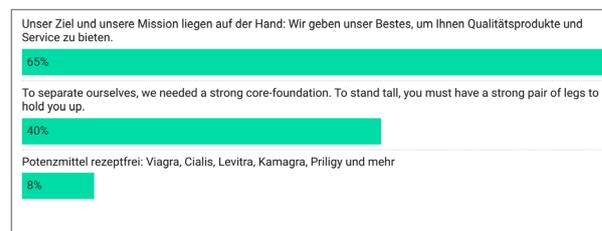


Abb. 10 Je nach Phrase waren die Ergebnisse des Crawlers unterschiedlich. Die Trefferquote liegt zwischen 8% und 65%.

Die Überwachung der WHOIS-Daten mithilfe des Scamadviser-Analysetools lieferte insgesamt 95 Domains, wobei hier rund 92% der gelieferten Ergebnisse tatsächlich betrügerisch waren. Zusätzlich bietet das Analysetool die Möglichkeit, Ergebnisse mit deutschsprachigen Tags auszuspielen. Dadurch kann die Relevanz für österreichische Konsument:innen sichergestellt und so irrelevante Ergebnisse herausgefiltert werden.

Das Crawling der Meta-Werbebibliothek hatte beim Auffinden von betrügerischen Versandapotheken keine Relevanz. Bereits die manuellen Tests zeigten, dass keine passenden Textphrasen gefunden werden konnten. Auch die Suche nach den entsprechenden Produkten (z.B. Viagra, Cialis) lieferten nur wenige und nicht clusterbare Ergebnisse. Erst gegen Ende des Analysezeitraum im September 2023 tauchten Werbeanzeigen für verschreibungspflichtige Arzneimittel häufiger auf: Im Zuge der (auch medial geführten) Diskussion rund um Diabetes-Medikamente (Ozempic, Wegovy, Saxenda etc.), die zur Gewichtsreduktion eingesetzt werden und von Lieferengpässen betroffen waren, tauchten entsprechende Fake-Shops (inkl. Meta-Werbeanzeigen) auf.²⁷ Diesbezüglich gilt es weiter zu beobachten, ob Produkte, die im BASG-Register von Vertriebsbeschränkungen²⁸ gelistet sind, auch vermehrt in der Meta-Werbebibliothek zu finden sind.

26 BNF (2022)

27 Watchlist Internet (2023b)

28 <https://medicineshortage.basg.gv.at/vertriebseinschraenkungen/>, zuletzt aufgerufen 21.12.2023

Qualitative Ergebnisse

Von allen gefundenen betrügerischen Online-Apotheken wurden neun für den deutschsprachigen Raum relevante Websites²⁹ ausgewählt und näher analysiert. Im Gegensatz zum Anlagebetrug und zum Betrug mit Nahrungsergänzungsmittel war in diesem Bereich aufgrund der zahlreichen Ergebnisse eine weitere Filterung der Ergebnisse nach Relevanz notwendig. Dafür wurde nach einem IETF-Sprachtag (z.B. lang="de") im Quellcode gesucht, um so auf für den deutschsprachigen Raum relevante Ergebnisse zu kommen. Zusätzlich gaben Meldungen, die an die Watchlist Internet gingen, sowie generelle Beschwerden zur jeweiligen Domain, einen Hinweis darauf, ob die Seite tatsächlich aufgerufen wird. Heraus kristallisiert hat sich schließlich ein Fokus auf Potenzmittel (bzw. auch andere verschreibungspflichtige Medikamente) und Steroide.

Da vor allem Betreiber:innen der ersten Kategorie als Versandapotheken auftreten, ist im Folgenden von Versand- oder Onlineapotheken die Rede, wenn der Schwerpunkt auf Potenzmitteln und anderen rezeptpflichtigen Arzneimitteln liegt, und von Online-Shops, wenn der Schwerpunkt auf Steroiden & Anabolika liegt. Folgende Websites wurden schließlich ausgewählt (siehe Abb. 13). Im Rahmen einer Web Content Analyse wurden Produktsortiment, Preispolitik, Zahlungsmöglichkeiten, Kundenorientierung und Kommunikation der Websites untersucht.

Produktangebot

Alle untersuchten betrügerischen Internetapotheken boten Potenzmittel verschiedener Marken an (in fünf davon ausschließlich Potenzmittel - meist für Männer). Der Fokus auf Medikamente gegen Erektionsstörungen spiegelt sich auch in der visuellen Gestaltung der Websites wider: Hinzu kommen Überschriften wie „Qualitätsprodukte für die Potenz“, Domainnamen wie „onlinepotenz.com“ oder „potenzmittelkaufenonline.com“.



Abb. 12 Screenshot illegalen Versandapotheken onlinepotenz.com.

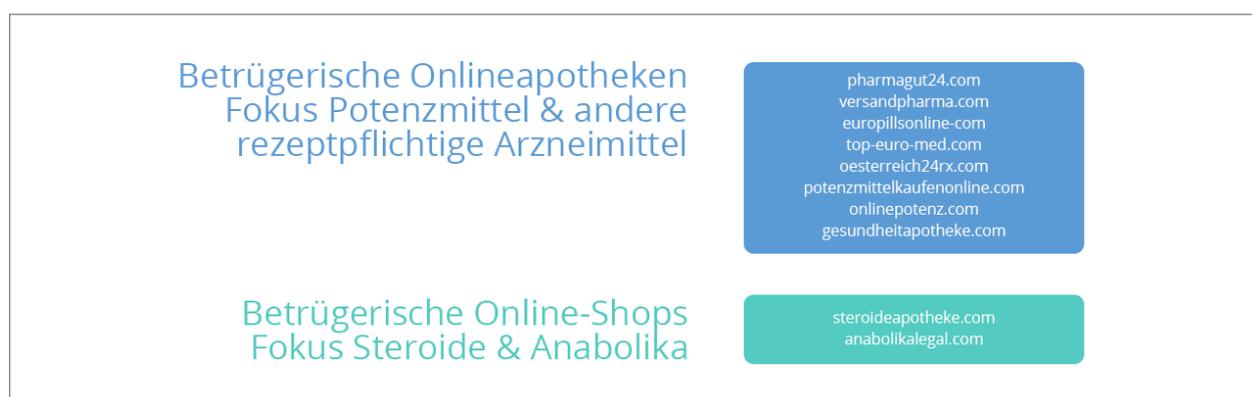


Abb. 11 Ausgewählte Websites für Web-Content-Analyse nach Kategorie.

²⁹ pharmagut24.com, versandpharma.com, europillsonline.com, top-euro-med.com, oesterreich24rx.com, potenzmittelkaufenonline.com, onlinepotenz.com, gesundheitapotheke.com, steroidapotheke.com, anabolikalegal.com.

Liegt der Fokus nicht auf Potenzmittel (das ist auf drei der Websites der Fall), wird z. B. durch Untertitel wie „Pillen ohne Rezept“ oder „Medikamente ohne Rezept“ dafür geworben, dass verschreibungspflichtige Medikamente ohne Rezept bestellt werden können. Die Produktpalette reicht dabei von Antidepressiva und Schmerzmitteln über Mittel gegen Haarausfall und Gewichtsverlust bis hin zu Medikamenten gegen Krebs, Diabetes, Asthma und andere, zum Teil schwerwiegende Erkrankungen.

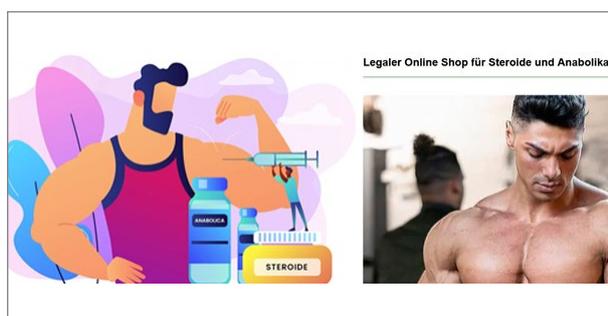


Abb. 13 Screenshots der Websites steroideapotheke.com und anabolikalegal.com.

In den Online-Shops für Anabolika werden Anabolika in Form von Spritzen und Tabletten verkauft. Darüber hinaus finden sich im Produktangebot Wachstumshormone, Testosteron, Östrogenblocker, Peptide, Fatburner sowie teils Potenzmittel – in diesem Fall zur Vermeidung von Nebenwirkungen durch die Einnahme von Anabolika.

Grafisch sind auch diese Shops auf Männer ausgerichtet, allerdings wird eine jüngere Zielgruppe angesprochen.

Preispolitik

Da in fast allen untersuchten Online-Apotheken das Produkt „Viagra (Original, 100mg)“ verkauft wird, wurde der Stückpreis dieses Produktes in den betrügerischen Shops mit dem Stückpreis in einer seriösen deutschen Online-Apotheke verglichen. In beiden Fällen legten wir dafür die Mindeststückanzahl in den Warenkorb.³⁰

Das Ergebnis: Die betrügerische Konkurrenz unterbietet die Preise des seriösen Anbieters (shop-apotheke.com) deutlich. Während die seriöse Versandapotheke Stückpreise von 18,80 Euro verlangt, schwanken die Preise auf den Betrugsseiten zwischen 6,71 Euro und 13,05 Euro.

Zu den günstigen Preisen, kommen Mengenrabatte dazu, die beim gesamten Bestellprozess an verschiedenen Stellen beworben werden – bspw. bei der Produktauswahl, aber auch im Warenkorb finden sich Hinweise darauf, dass bei einer größeren Bestellung günstigere Stückpreise möglich sind. Auch zusätzliche Rabattaktionen oder Treueprämien werden angepriesen.

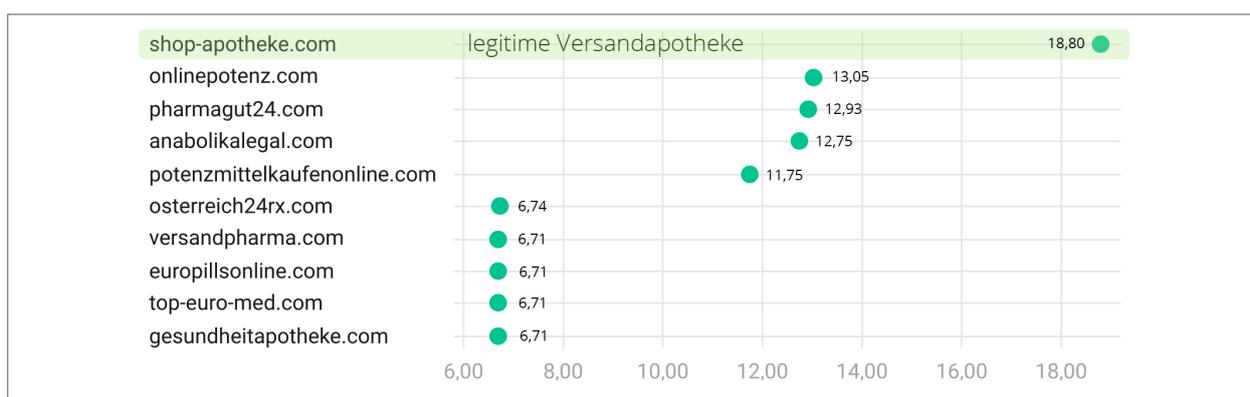


Abb. 14 Stückpreis des Produkts „Viagra (Original, 100mg)“ beim Mindesteinkauf von 4 Stück.

30 Der Vergleich mit einer österreichischen Online-Apotheke war nicht möglich, da in Österreich keine rezeptpflichtigen Arzneimittel online verkauft werden dürfen.

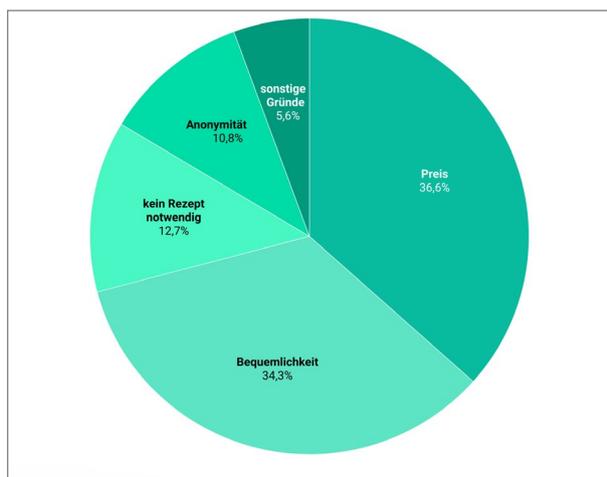


Abb. 15 Gründe, warum Menschen Arzneimittel im Internet kaufen, Projekt Fakecare, eigene Darstellung.

Dieses Preisdumping ist besonders problematisch, wenn man einen Blick auf die Motivation von Konsument:innen wirft, Medikamente online einzukaufen. Eine Umfrage, die vom EU-geförderten Projekt „Fakecare“ (2016) in sieben EU-Ländern durchgeführt wurde, zeigt, dass 36,6 % der Befragten von günstigeren Preise und Sonderrabatten angelockt werden.³¹

Kunden-Orientierung

Die Umfrage des Projekts Fakecare zeigt auch, dass Anonymität (10,8 %) sowie die Möglichkeit Medikamente ohne Rezept zu bestellen (12,7 %), Gründe dafür sein können, Arzneimittel online zu bestellen.³² Auch das spiegelt sich auf den Fake-Seiten wider: Geworben wird nicht nur damit, dass trotz verschreibungspflichtiger Medikamente kein Rezept notwendig ist, sondern auch die Kundenorientierung wird in den Vordergrund gestellt, Diskretion und Anonymität werden versprochen („Sicher und Zuverlässig“, „Schnelle und sichere diskrete Lieferung“, „Qualität und Diskretion“ etc.).

Zahlung

Die Bedeutung einer anonymen Bestellung zeigt sich auch bei den Zahlungsarten. So bieten viele Versandapotheken die Zahlung per Kreditkarte an, wenige Websites ermöglichen Überweisungen, die

meisten setzen neben der Kreditkarte auf Kryptowährungen (Bitcoin und Ethereum). Damit die Zahlung mit Kryptowährungen auch genutzt wird, werden Vorteile angeboten: Wer Bitcoin oder Ethereum wählt, bekommt 10 Prozent auf den Warenkorb gutgeschrieben. Die Vermutung liegt nahe, dass hier nicht nur die Anonymität gegenüber den Kund:innen, sondern auch jene der Website-Betreiber:innen gewährleistet werden soll.

Kontakt & Kommunikation

Die Identität der Apothekenbetreiber wird, wenig überraschend, auch bei den Angaben auf den Websites verschleiert: Das in Österreich vorgeschriebene Impressum sucht man auf den Seiten vergeblich, eine Adresse wurde nur in einem Fall gefunden (übernommen von einer legitimen Apotheken in Dortmund).

Dennoch gibt es verschiedene Möglichkeiten die Apotheken zu erreichen: Neben Kontaktformularen, E-Mail-Adressen sowie die Möglichkeit über Messenger wie Viber, Telegram oder WhatsApp in Kontakt zu treten, sind auch Telefonnummern auf den Seiten angegeben. Meist sind dabei mehrere Nummern angegeben, denn auch diesbezüglich wird Kundenorientierung groß geschrieben – es sind Telefonnummern für viele Länder (US, UK, DE, CH, AT) angegeben. Alle gefundenen Telefonnummern waren gültig, wobei die Nummern aus DE, CH und AT von seriösen Apotheken kopiert wurden. Bei den Telefonnummern aus den USA und aus UK konnten wir die gleiche Nummer auf verschiedenen Seiten finden. Ein Hinweis darauf, dass einige der betrügerischen Versandapotheken vom gleichen Netzwerk betrieben werden.

Eine weitere Kontaktmöglichkeit sind Live-Chats. Wir haben alle verfügbaren Live-Chats ausprobiert und dabei unser Unbehagen über die Qualität der Lieferung und die Seriosität der Versandapotheke zum Ausdruck gebracht.

Beruhigt wurden wir mit unterschiedlichen

31 Mignone (2016)
32 Ebenda

Strategien:

- **Unwahre Behauptungen:** Produkte sind von der FDA zugelassen und/oder entsprechen allen notwendigen Richtlinien, der niedrige Preis erklärt sich durch den Verkauf von Generika (obwohl es um Original-Viagra ging).
- **Verweis auf Ärzt:innen:** Bei medizinischen Fragen wurde uns geraten einen Arzt zu konsultieren, bevor bestellt wird.
- **Frage bleibt unbeantwortet:** Statt die Frage zu beantworten werden Informationen zu Lieferung und Versand gegeben, solche Standard-Fragen (nach Skript) zu beantworten, scheint die einzige Funktion der Chats zu sein.

Auffällig war zudem, dass die Chat-Agent:innen, die wir über unterschiedliche Shops kontaktiert haben, teils wortwörtlich, teils mit leichten Abwandlungen, die gleichen Antworten gaben. Auch der Name eines Chat-Agenten begegnete uns mehrmals auf unterschiedlichen Websites.

Eine Ausnahme von dieser Wortkargheit stellt einer der Online-Shops zu Steroiden dar: Ein Shop, der sich nicht nur durch einen deutlich professionelleren Online-Auftritt, sondern auch durch eine Beratung und durch Empfehlungen per Live-Chat hervortut.

Hier ein Auszug aus dem Chat:

ÖIAT: Ich bin mir unsicher, ob oral oder eine Injektion für mich in Frage kommt. Was sind denn da die Vor- und Nachteile?

Alex (Berater): Oral bringt weniger Wirkstoff als Injection in den Körper

ÖIAT: Aber kann das auch gefährlich sein?

ÖIAT: Also die Injektion? Eine Spritze klingt so heftig irgendwie :/

Alex (Berater): Bodybuilder spritzen sich den Tag lang irgend etwas rein zum Frühstück, Nachmittag und Mittagschlaf und alles so weit gut.

[...]

ÖIAT: Ich sehe grad, dass es da unterschiedliche Anbieter von den gleichen Anabolika gibt. Also zum Beispiel Balkan Pharmaceuticals, Pharmacom Labs und so. Was ist denn da der Unterschied?

ÖIAT: Alex, sind Sie noch hier?

Alex (Berater): Ja sorry habe viel zu tun

Alex (Berater): das sind alle gute Hersteller zu verschiedenen preisen

Alex (Berater): Ich empfehle Balkan, Elbrus, Magnus

ÖIAT: Und die Lieferzeit ändert sich da auch nicht? Oder woher wird das dann geliefert?

Alex (Berater): aus DE die Lieferung mit Verpackung dauert von 1 – 2 Wochen

ÖIAT: Ah super, Ihr Lager ist in Deutschland.

ÖIAT: Eine etwas persönliche Frage: Nehmen Sie selbst Anabolika oder worauf basieren Ihre Empfehlungen?

Alex (Berater): Habe früher als ich trainiert habe aber jetzt ist mein Körper in der Form in der ich ihn haben will deswegen brauche ich das nicht mehr

ÖIAT: Wow! Auch noch jemand, der sich auskennt hier im Kundensupport. Ich bin begeistert. :D

ÖIAT: Nochmal wegen der Frage zu oral vs. Injizieren: Haben Sie auch medizinisches Personal, die mir dabei helfen das beste Produkt für mich auszusuchen?

Alex (Berater): Die sind sehr Teuer bei uns und nur für Profis gedacht die zu Mr Olympia sich vorbereiten

Alex (Berater): aber ich kann Ihnen helfen

Insgesamt präsentiert sich die Website anabolikalegal.com als professioneller Online-Shop mit Expertise im Bereich Anabolika: So kann der „Sportpharmakologe“ und „Ernährungsberater“ Sergey Ivanov per Messenger kontaktiert werden (gemeint ist möglicherweise „das teure medizinische Personal“). Auf der Website finden sich Zertifikate, die die Expertise beweisen sollen, genauso wie Stellenangebote (Lagerist, Provisorium und Verkaufsleiter) sowie Links zu Seiten, auf denen der Authentifizierungscode der Medikamente überprüft werden kann.

Nicht ganz so professionell wirkt die Website steroideapotheke.com, aber auch hier vermitteln Blogbeiträge und die Kommunikation den Eindruck, dass die Betreiber aus der Szene kommen oder zumindest mit ihr in Kontakt stehen.

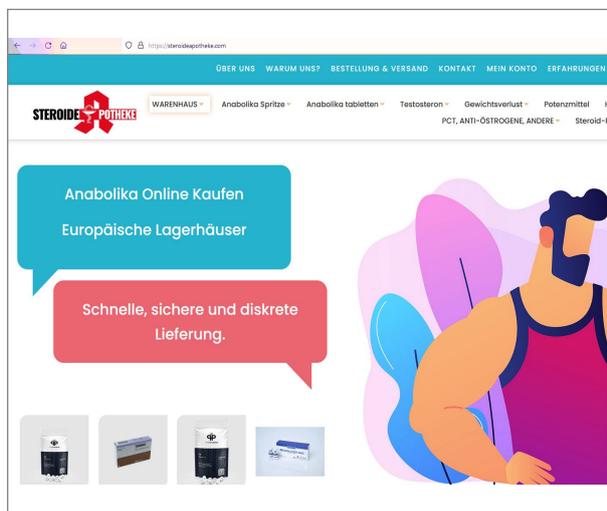


Abb. 16 Screenshot steroideapotheke.com.

RX-App

Es wurde bereits angedeutet, dass es sich bei den für Österreich als relevant eingestuften Online-Apotheken zum Teil um dieselben Anbieter handeln könnte. Diese Vermutung wird durch das Angebot der „RX-App“ bestätigt, die auf einigen der Websites beworben wird.

Auf der Website rxappfree.com kann die App über einen QR-Code heruntergeladen werden. Auch das ist ein Service für hervorragende Kundenorientierung, speziell für Stammkund:innen. So können in der App nicht nur Produkte bestellt und mit einem Klick nachbestellt („one click order“), sondern auch Erinnerungen zur zeitgerechten Medikamenteneinnahme eingestellt werden.

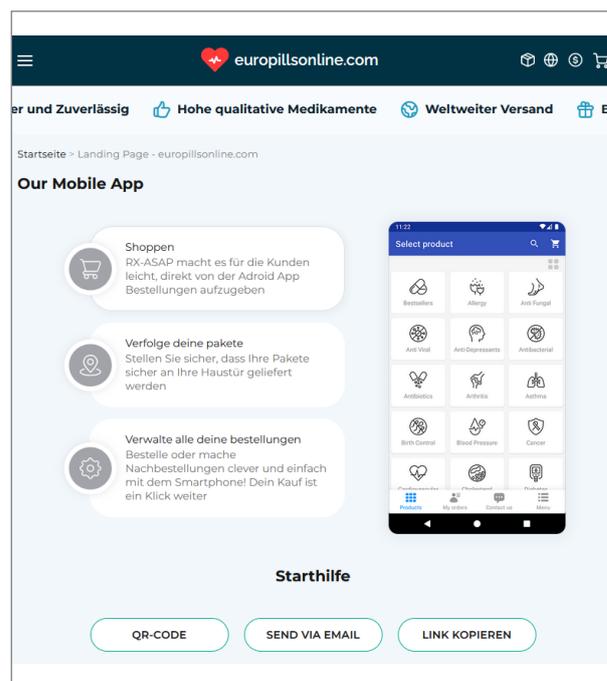


Abb. 17 Bewerbung der RX-App auf europillsonline.com

Weitere strukturelle Merkmale

Es zeichneten sich durch diese Analyse folgende Muster ab, die sowohl Konsument:innen als Anhaltspunkte zum Entlarven betrügerischer Seiten dienen als auch weitere Forschungsprojekte in der Detektion von Medikamentenbetrug speisen können:

- **Kein Rezept notwendig:** In Österreich ist es verboten verschreibungspflichtige Medikamente online zu verkaufen. Fake-Apotheken setzen ganz gezielt auf verschreibungspflichtige Produkte, vor allem Potenzmittel, aber auch auf Trends wie die Einnahme von Diabetesmedikamente als Schlankheitsmittel konnten im Zuge der Recherche identifiziert werden.
- **Fehlendes Impressum:** Keine der Websites hatte ein Impressum, ein solches ist in Österreich jedoch verpflichtend.
- **Erklärungen zu Generika:** Viele betrügerische Websites betonen im Gegensatz zu legitimen Versandapotheken den Verkauf von Generika (auch wenn viele Markenprodukte verkauft werden) und liefern ausschweifende Erklärungen dazu. In den Live-Chats wurde klar, dass dieser Fokus dabei hilft, Dumping-Preise zu rechtfertigen.
- **Rechtschreibung, Grammatik und Sprachenmix:** Insbesondere deutschsprachige Fake-Apotheken zeichnen sich durch besonders viele Rechtschreib-, Grammatikfehler sowie einen Sprachenmix (meist Deutsch und Englisch) aus.
- **Weltweiter Versand und andere Versprechungen:** Auf den Websites sind Schlagwörter wie zum Beispiel „sicher und zuverlässig“, „weltweiter Versand“, „sicher und diskret“ hervorgehoben.
- **EU-Sicherheitslogo:** In jedem Land der europäischen Union gibt es eine Liste registrierter Versandapotheken.³³ In Österreich ist dafür die BASG zuständig.³⁴ Ähnliche Register anderer EU-Länder finden Sie auf der Seite der Europäischen Arzneimittel-Agentur: Auf der Website der Apotheken selbst werden registrierte und damit legitime Anbieter durch das EU-Sicherheitslogo ausgewiesen. Dieses muss zusätzlich anklickbar sein und zur nationalen Arzneimittel-

behörde führen.

Für zukünftige Forschungsprojekte gilt es zu überlegen, wie mit den gefundenen Merkmalen weitere Detektionsmethoden entwickelt bzw. bestehende Methoden verfeinert werden können: Dazu zählt bspw. das Einspeisen von Begriffen, die auf eine Umgehung der Rezeptpflicht abzielen („rezeptfrei“, „ohne Rezept“). Da diese Begriffe einen eindeutigen Hinweis auf Betrug darstellen, könnte so die manuelle Bewertung erleichtert werden. Das Scraping von Impressums- und Kontaktdaten sowie die Suche nach diesen Daten, sofern diese gefunden wurden, kann die Bewertung durch die Vergabe von Risikoscores erleichtern (keine Impressumsdaten oder Kontaktdaten, die auch auf anderen Betrugsseiten zu finden sind, würden z.B. zu einem hohen Risikoscore führen).

Eine weitere Entwicklung, die die manuelle Qualitätssicherung erleichtern würde, ist die automatisierte Filterung der Ergebnisse durch Relevanzanalysen. Im Rahmen des Forschungsprojekts wurden die zahlreichen Treffer manuell durch eine Suche nach Sprachtags ermittelt. Eine Automatisierung dieser Suche in Kombination mit Traffic-Analysen würde den Bearbeitungsaufwand deutlich reduzieren.

³³ <https://www.ema.europa.eu/en/human-regulatory-overview/public-health-threats/falsified-medicines-overview/buying-medicines-online>, zuletzt aufgerufen 21.12.2023

³⁴ BASG (2023)

Nahrungsergänzungsmittel

Begriffsbestimmung

Nahrungsergänzungsmittel (NEM) sind Lebensmittel für bestimmte Zielgruppen, die aus einer ernährungswissenschaftlichen Perspektive, als nicht notwendig, jedoch als teilweise sinnvoll für bestimmte Lebensumstände gelten, z. B. bei Kinderwunsch, Leistungssport oder chronischen Schmerzen. Die Bandbreite der Produkte, die als NEM gilt, reicht von Vitaminen hin zu Mahlzeitsurrogaten oder Kräutern. Ihre Kategorisierung kann entlang der Anwendungsgebiete (Immunsystem, Bewegungsapparat, Schönheit, Gehirn/Nerven, Frauen- o. Männergesundheit, Herz-Kreislauf, Sport, Augen) oder entlang der typischen Inhaltsstoffe (Abbildung 19) vorgenommen werden. Im Unterschied zu Lebensmitteln müssen NEM eine ernährungsspezifische oder physiologische Wirkung haben und als Konzentrate in kleinen, dosierten Mengen oral eingenommen werden. Sie unterliegen nicht dem Arzneimittelgesetz.

NEM werden dabei zunehmend digital vertrieben. Bereits 2020 wickelte über ein Drittel der Käufer:innen ihre Bestellung online ab.³⁵ Diese Digitalisierung der Vertriebswege geht auch mit zunehmenden Betrugsversuchen rund um Nahrungsergänzungsmittel einher. Dabei richten Kriminelle betrügerische Online-Shops ein, um unterschiedliche Produkte zu verkaufen und diese gleichzeitig als Wundermittel zu vermarkten.

Health Claims Verordnung

Allein durch eine solche Vermarktung verstoßen die Shop-Betreiber:innen gegen die sogenannte Health Claims Verordnung: Nach der „Verordnung über nährwert- oder gesundheitsbezogene Angaben (EG) Nr. 1924/2006“³⁶ sind Aussagen, die darauf hinweisen, dass ein Nahrungsergänzungsmittel der Vorbeugung, Behandlung oder gar der Heilung einer Krankheit dient, verboten. NEM sind schließlich Lebensmittel und keine Medikamente.



Abb. 18 Klassifikation nach typischen Inhaltsstoffen von Nahrungsergänzungsmitteln.

35 Österreich - Einnahme von Nahrungsergänzungsmitteln 2021 o.A. (2023)

36 Regulation (EC) No 1924/2006 of the European Parliament and of the Council of 20 December 2006 on nutrition and health claims made on foods (2014)

Zugelassen sind ausschließlich gesundheitsbezogene Angaben (und keine krankheitsbezogene Angaben), die behördlich zugelassen wurden. Von 44.000 Autorisierungsanfragen (seit 2008) waren allerdings nur 229 erfolgreich, meist Vitamine. Nur diese zugelassenen Aussagen dürfen von Herstellern oder Händlern für die gesundheitsbezogene Kennzeichnung und/oder beim Vertrieb verwendet werden.

Unklare Inhaltsstoffe

Während die Online-Bewerbung und der Vertrieb (kommt ein Produkt an oder nicht?) sowohl vom Projektteam als auch vom Team der Watchlist Internet bewertet werden kann, ist es schwierig, darüber hinausgehende Aussagen zu treffen. Klar ist, dass in den meisten Fällen tatsächlich Produkte ankommen. Eine wesentliche Frage bleibt jedoch unbeantwortet: Handelt es sich bei den gelieferten Nahrungsergänzungsmitteln, um ein wirkungsloses Produkt, das überteuert verkauft wurde. Oder enthält das Produkt nicht deklarierte pharmakologische Inhaltsstoffe, die zwar eine Wirkung zeigen, gleichzeitig aber die Gesundheit der Konsument:innen gefährden können. Die Relevanz und die Gefahr, die von dieser Art von Betrug ausgeht, sind daher schwer einzuschätzen.

Einen Hinweis auf die Problemlage gibt jedenfalls die Website der gemeinnützigen GmbH „Gute Pillen – Schlechte Pillen“ (GPSP), die bis 2020 eine Datenbank mit Nahrungsergänzungsmitteln und Arzneimitteln führte, die mit nicht deklarierten Arzneistoffen „gepanscht“ waren. Als besonders problematisch bewertet GPSP dabei „natürlich“ beworbene Produkte, in denen Wirkstoffe wie Sildenafil, Sibutramin oder Fluoxetin zu finden waren.³⁷

Abgrenzung zum legitimen Markt

Sowohl die Unklarheit darüber, ob Konsument:innen mit gefährlichen Inhaltsstoffen konfrontiert sind als auch die Probleme rund um die Health Claims Verordnung, tragen dazu bei, dass eine klare Abgrenzung zum seriösen Markt nicht immer möglich ist.

Denn es gibt auch legitime Anbieter:innen, die die Health Claims Verordnung – wissentlich oder nicht – missachten. Teils werden gesetzliche Regulierungen auch ganz bewusst versucht zu umgehen, beispielsweise indem die heilende Wirkung durch den Produktnamen oder visuell suggeriert wird oder der Verkauf über Online-Shops mit Sitz außerhalb der EU erfolgt.

So zeigt der Lebensmittelsicherheitsbericht 2022 der Österreichischen Agentur für Ernährung und Gesundheit (AGES), dass von den insgesamt 310 begutachteten Produkten 27% beanstandet wurden. In den meisten Fällen handelte es sich um Kennzeichnungsmängel sowie irreführende Angaben.³⁸ Ähnliche Probleme bestätigt auch die erste europaweit koordinierte Kontrolle von online angebotenen Lebensmitteln der EU-Kommission: Von 1.100 Websites wurden insgesamt 779 Produktangebote gefunden, die nicht verkehrsfähig waren, wobei auch hier der Schwerpunkt auf gesundheitsbezogenen Angaben lag.³⁹ Sowohl in der europaweiten Kontrolle als auch im Lebensmittelsicherheitsbericht 2022 wurde der Fokus nicht auf kriminelle Akteur:innen gelegt, sondern u.a. legitime Marktteilnehmer:innen kontrolliert.

Quantitative Analyseergebnisse

Um betrügerische Anbieter:innen von Nahrungsergänzungsmitteln ausfindig zu machen, wurde die Überwachung der Google Analytics ID (siehe Kapitel 2.1.) ebenso angewandt wie das textbasierte Crawling. Das textbasierte Crawling der Google Suchmaschine lieferte dabei kaum Ergebnisse (43). Die Gründe hierfür liegen zum einen in der Cloaking-Problematik, zum anderen in der textlichen „Kreativität“ der Kriminellen. So zeigten die Recherchen, dass im NEM-Bereich Phrasen nicht unbedingt 1:1 übernommen werden, sondern diese von Shop zu Shop leicht angepasst werden.

Schnell klar wurde hingegen, dass Kriminelle, die im NEM-Bereich tätig sind, auf die Bewerbung ihrer Produkte über Social Media setzen. Dementspre-

37 <https://gutepillen-schlechtepillen.de/gepanschtes/>, zuletzt aufgerufen 21.12.2023

38 Lebensmittelsicherheitsbericht - KVGöA (2023)

39 Europäische Kommission (2018)

chend ergiebiger war das Crawling der Meta-Werbebibliothek. Gesucht wurde dabei hauptsächlich nach Produktnamen. Zum Beispiel nach dem von Kriminellen massiv beworbenen Abnehmprodukt „KetoXplode“. Allein für die Monate September bis November 2023 konnten wir mit dem Suchbegriff „ketoxplode“ rund 430 Anzeigen ausfindig machen. Die Zielgruppe ist dabei überwiegend weiblich, zwischen 24 und 65 Jahren und lebt in Österreich und Deutschland. Pro Werbeanzeige wurde eine Reichweite von mehreren hundert bis zu tausenden Personen in Österreich erzielt.

Ein weiteres Beispiel ist Gluconol, ein angebliches Diabetesmittel, das vom Bundesamt für Sicherheit im Gesundheitswesen (BASG) als illegal eingestuft wurde.⁴⁰ Über die Meta-Werbebibliothek konnten wir zwischen September und November 2023 rund 200 betrügerische Anzeigen ausfindig machen.

Qualitative Analyseergebnisse

Aufgrund der schwierigen Einstufung der Ergebnisse als Betrug sowie der Unmöglichkeit die Risiken für Konsument:innen zu bewerten, wurden nur drei Produkte detailliert analysiert, bei denen die Betrugsabsicht aufgrund verschiedener struktureller Merkmale, die auch von anderen Betrugsseiten bekannt sind, oder aufgrund bereits gemachter Erfahrungen in dem Bereich vonseiten der Watchlist Internet, eindeutig war. Bei den Produkten handelt es sich um Mittel gegen Bluthochdruck (Cardione), gegen Diabetes (Gluconol) und zum Abnehmen (KetoXplode), die jeweils mit mehreren betrügerischen Online-Shops verknüpft sind. Das Ergebnis: Alle drei Produkte werden auf ähnliche Weise beworben und vertrieben. Folgende Muster, die sich mit den Erfahrungen der Watchlist Internet decken, sind dabei zentrale Erkennungsmerkmale des Betrugs:

- Bewerbung mit Fake-Newsartikel
- Fokus auf ein Produkt
- Empfehlungen von Ärzt:innen
- Fehlendes Impressum/Sitz außerhalb EU
- Angabe von Telefonnummern

Bewerbung durch Fake-Newsartikel

Ähnlich wie im Falle von betrügerischen Tradingplattformen erfolgt die Bewerbung auch häufig über Fake-Newsartikel. Meist werden hierfür nicht Prominente, sondern Bilder und Namen von Ärzt:innen missbraucht, um die Richtigkeit der getroffenen Aussagen zu unterstreichen. Dabei werden die genannten NEM als Wundermittel vermarktet, entsprechend lassen sich zahlreiche Verstöße gegen die Health Claims Verordnung feststellen. Mit Heilsversprechen („Prävention von Hirnschlägen“, „100% LESS BAD CHOLESTERIN“, „Diabetes für immer weg“) wird auf die Verzweiflung besonders gefährdeter Personengruppen gesetzt.

Wie bereits dargestellt, ist es nicht möglich, Produkte ohne Labortests auf Risiken zu untersuchen. Dennoch zeigt sich jedenfalls eine gesundheitliche Gefahr durch die Aussagen der Kriminellen, die vor allem in den Newsartikeln getroffen werden. Gluconol beispielsweise wird nicht nur als Diabetes-Wundermittel beworben, Kriminelle rufen zusätzlich dazu auf, die von Ärzt:innen verschriebenen Diabetesmedikamente nicht mehr einzunehmen, da diese schädlich – sogar tödlich – seien.



Abb. 19 Ein Fake-Newsartikel, der Gluconol bewirbt und andere Diabetesmittel als tödlich benennt.

40 BASG (2022)

Im Fall von „KetoXplode“ drehen sich die Fake-Newsartikel meist um die Fernsehsendung „Die Höhle der Löwen“, in der das unglaubliche Produkt vorgestellt wurde. „Vor dem Schlafengehen einnehmen. Am dritten Tag passte die Hose nicht mehr“, lautet eine der Phrasen, mit denen das Nahrungsergänzungsmittel dabei beworben wird. Auch solche Aussagen verstoßen gegen die Health Claims Verordnung.

Fokus auf ein Produkt

Entscheiden sich Konsument:innen für den Kauf des Produktes, werden sie in der Regel auf die entsprechenden Websites weitergeleitet, auf denen nur ein einziges Produkt, nämlich das jeweilige Nahrungsergänzungsmittel, verkauft wird. Auf der Seite wird die Bewerbung des Nahrungsergänzungsmittels, als „natürlich“ und gleichzeitig als einzig funktionierendes Heilmittel ein weiteres Mal betont.

Empfehlungen von Ärzt:innen

Ärzt:innen werden auch auf den Websites genutzt, um die Vertrauenswürdigkeit in das jeweilige NEM zu erhöhen und die getroffenen gesundheitsbezogenen Aussagen als wissenschaftlich anerkannt darzustellen.



Abb. 20 Der „Arzt“ Manuel Feiertag empfiehlt „Cardione-Tabletten“ gegen hohen Blutdruck

Auf ketoexplode.at wird zudem behauptet, dass eine „individuelle Prognose“ für die Gewichtsabnahme

erstellt wird: „Die KETOXPLODE-Anwendung ist erfolgreich und durch Studien belegt. Auf dieser Datengrundlage können wir die Zeit berechnen, die Sie für die Erreichung Ihres gewünschten Gewichts vermutlich benötigen“, heißt es auf der Website. Zusätzlich kommen auf einigen Websites auch angebliche „Konsument:innen“ zu Wort und berichten von der angeblichen Wirkung des jeweiligen Nahrungsergänzungsmittels.

Fehlendes Impressum oder Sitz außerhalb EU

Wie die Erfahrungen der Watchlist Internet und die analysierten Websites zeigen, fehlt meist ein Impressum. Selten wird auch ein Impressum angegeben, der Sitz des Unternehmens ist in diesen Fällen im EU-Ausland – so ist auf ketoexplode.com eine Adresse im Vereinigten Königreich angegeben. Die Existenz des Unternehmens (Dohobue LTD) konnte nicht bestätigt werden. Stattdessen ergab eine Recherche, dass mit denselben Unternehmensdaten zahlreiche weitere Websites betrieben werden, auf denen Abnehm- und andere Wundermittel verkauft werden. Darunter auch diaetolin.com, ein Abnehm-mittel vor dem die Watchlist Internet bereits seit Anfang 2023 warnt, damals war im Impressum noch ein anderer Unternehmensnamen zu finden.⁴¹

Abfrage von Telefonnummern

In der zweiten Jahreshälfte 2023 ließ sich ein Trend dahin erkennen, dass – ähnlich dem Verlauf von Kryptobetrug – Telefonnummern abgefragt werden. In solchen Fällen werden Konsument:innen nicht unbedingt von den Fake-Newsartikeln weitergeleitet, das Bestellformular ist am Ende des Berichts eingebettet und kann direkt dort ausgefüllt werden. Wird die Telefonnummer abgefragt (sowohl auf Websites als auch in Fake-Newsartikeln), ist dieses Feld ein Pflichtfeld. Wir vermuten, dass diese Vorgehensweise insbesondere eine ältere Zielgruppe ansprechen soll, die solche Geschäfte lieber telefonisch abwickelt.

41 Watchlist Internet (2023c)

Ausblick

Die Untersuchung von betrügerischen Websites offenbart Muster in verwendeten Texten und Strukturen, da viele der analysierten Seiten zu kriminellen Netzwerken gehören, bzw. von denselben Personen betrieben werden. Automatisierte Detektionsmethoden, insbesondere der Einsatz von Web-Crawlern, bieten die Möglichkeit, die Vielzahl betrügerischer Domains zu identifizieren und Konsument:innen rechtzeitig vor diesen Angeboten zu warnen.

Unterschiedliche Crawling-Methoden wurden auf ihre Eignung zur Identifizierung betrügerischer Tradingplattformen, Versandapotheken und Online-Shops für Nahrungsergänzungsmittel getestet. Beispiele hierfür sind das Crawling von HTTP-Transaktionen, das Überwachen von Google Analytics ID, die Überwachung von Backlinks, WHOIS-Daten, Redirects, sowie textbasiertes Crawling der Google-Suchmaschine und der Meta-Werbebibliothek. Die Suche nach Textphrasen über Google und das Crawling der Meta-Werbebibliothek adressieren spezifischere Aspekte, erfordern jedoch eine präzise Auswahl von Begriffen und eine zeitaufwändige manuelle Überprüfung der generierten Ergebnisse.

Über die sehr diversen Themenbereiche von Cyber-Trading-Fraud (betrügerische Tradingplattformen), betrügerische Versandapotheken und Nahrungsergänzungsmittel konnte eine Vielzahl an Methoden für das Auffinden von betrügerischen Websites erprobt und verbessert werden. So bietet Fraud Seeker einen optimalen Startpunkt für die Weiterentwicklung und das Deployment der entwickelten Tools im Alltagsgeschäft der Watchlist Internet.

Insgesamt wurde durch das Projekt Fraud Seeker klar, dass eine Kombination unterschiedlicher Crawling-Methoden notwendig ist, um betrügerische Websites effektiv zu identifizieren und Konsument:innen rechtzeitig zu warnen. Automatisierte Ansätze können einen wichtigen Beitrag zur Betrugsprävention leisten, erfordern jedoch weiterhin manuelle Überprüfungen. Die fortlaufende Entwicklung und Anpassung von Crawling-Strategien sind entscheidend, um den sich ständig wandelnden Methoden der Kriminellen entgegenzuwirken.

Die Komplexität der Themen, vor allem Investmentbetrug, aber auch der Betrug mit Arzneimitteln und Nahrungsergänzungsmitteln verdeutlicht die Notwendigkeit von Kooperationen, wie z. B. mit Analselabors, um Produkte hinsichtlich ihrer Wirkung zu untersuchen. In diesem Bereich müssen neben der Risikoeinstufung auch die Präventionsmaßnahmen überdacht und neu konzipiert werden. Aktuell bergen Warnartikel vor falschen Gesundheitsversprechen die Gefahr, dass verzweifelte Personen ihre letzte Hoffnung auf diese Heilsversprechen setzen. Bestellung könnten so durch eine gut gemeinte Berichterstattung, weiter steigen.

Quellenangaben

- BASG (2022): Gluconol. 4.10.2022, URL: <https://www.basg.gv.at/marktbeobachtung/amtliche-nachrichten/detail/gluconol> [Zugriff: 4.12.2023]
- BASG (2023): Versandapotheken. 29.11.2023, URL: <https://www.basg.gv.at/konsumentinnen/arzneimittel-im-internet/versandapotheken> [Zugriff: 29.11.2023]
- BAVG (2023): Lebensmittelsicherheitsbericht - KVG. 2.11.2023, URL: <https://www.verbrauchergesundheit.gv.at/Lebensmittel/lebensmittelkontrolle/LMSicherheit.html> [Zugriff: 2.11.2023]
- BMF (2022): Produktpiraterieberichte an den Nationalrat und Aufgriffsstatistik. 2022, URL: <https://bmf.gv.at/themen/zoll/produktpiraterie/produktpirateriebericht-aufgriffsstatistik.html> [Zugriff: 27.1.2023]
- Chen, Zhouhan; Freire, Juliana (2021): Discovering and Measuring Malicious URL Redirection Campaigns from Fake News Domains. IEEE, URL: <https://ieeexplore.ieee.org/abstract/document/9474273/> [Zugriff: 13.12.2023]
- Europäische Kommission (2018): The first EU coordinated control plan on online offered food products Ref. Ares(2018)893577., URL: https://food.ec.europa.eu/system/files/2018-02/oc_oof_analysis_main_outcome_en.pdf
- IGEPHA - The Austrian Self Care Association (2023): Wo die Österreicher:innen ihre Medikamente kaufen. 2023, URL: <https://igepha.at/newsartikel/wo-die-oesterreicherinnen-ihre-medikamente-kaufen/> [Zugriff: 29.11.2023]
- LegitScript (2016): The Internet Pharmacy Market in 2016. 2016, URL: <http://safemedsonline.org/wp-content/uploads/2016/01/The-Internet-Pharmacy-Market-in-2016.pdf> [Zugriff: 24.2.2023]
- Mignone, Mara (2016): Project FAKECARE - Final Research Report.
- National Association of Boards of Pharmacy (2022): Rogue RX Activity Report. Disrupting Illegal Online Pharmacies: Lock and Suspend as a Tool to Protect Patients., URL: <https://nabp.pharmacy/wp-content/uploads/2022/10/Rogue-Rx-Activity-Report-Disrupting-Illegal-Online-Pharmacies-2022.pdf> [Zugriff: 12.4.2023]
- OECD; European Union Intellectual Property Office (2020): Trade in Counterfeit Pharmaceutical Products. OECD, URL: https://www.oecd-ilibrary.org/governance/trade-in-counterfeit-pharmaceutical-products_a7c7e054-en [Zugriff: 27.1.2023]
- Phillips, Ross; Wilder, Heidi (2020): Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites. In: 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 5.2020, S. 1–8
- Prieto, Juan Carlos; Fernandez-Isabel, Alberto; De Diego, Isaac Martin; Ortega, Felipe; Moguerza, Javier M. (2021): Knowledge-Based Approach to Detect Potentially Risky Websites. In: IEEE Access, Band 9, 2021, S. 11633–11643, URL: <https://ieeexplore.ieee.org/document/9321392/> [Zugriff: 14.2.2023]
- Regulation (EC) No 1924/2006 (2014): Regulation (EC) No 1924/2006 of the european parliament and of the council of 20 December 2006 on nutrition and health claims made on foods., URL: <http://data.europa.eu/eli/reg/2006/1924/2014-12-13/eng> [Zugriff: 7.11.2023]
- RIS (2023): Arzneimittelgesetz - Bundesrecht konsolidiert, Fassung vom 29.11.2023. 29.11.2023, URL: <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10010441&TabbedMenuSelection=BundesrechtTab> [Zugriff: 29.11.2023]
- Statista (2021): Österreich - Einnahme von Nahrungsergänzungsmitteln 2021. 2021, URL: <https://de.statista.com/statistik/daten/studie/1177629/umfrage/umfrage-zur-einnahme-von-nahrungsergaenzungsmitteln-in-oesterreich/> [Zugriff: 20.12.2023]
- Watchlist Internet (2020a): Zahlreiche neue Fake-Shops locken mit günstigen Angeboten und gutem Kundendienst. 2020, URL: <https://www.watchlist-internet.at/news/zahlreiche-neue-fakeshops-locken-mit-guenstigen-angeboten-und-gutem-kundendienst/> [Zugriff: 14.12.2023]
- Watchlist Internet (2020b): Achtung vor Shops mit service6@vinayotap.com E-Mail-Adressen. 2020, URL: <https://www.watchlist-internet.at/news/achtung-vor-shops-mit-service6-vinayotap-com-e-mail-adressen/> [Zugriff: 14.12.2023]
- Watchlist Internet (2023a): Fake-Shops geben sich als Shops für Warenhausaufösungen aus. 2023, URL: <https://www.watchlist-internet.at/news/fake-shops-geben-sich-als-shops-fuer-warenhauseaufloesungen-aus/> [Zugriff: 14.12.2023]
- Watchlist Internet (2023b): Ozempic, Wegovy & Co: Vorsicht vor Fake-Shops mit „Schlankheitsmitteln“. 2023, URL: <https://www.watchlist-internet.at/news/ozempic-wegovy-co-vorsicht-vor-fake-shops-mit-schlankheitsmitteln/> [Zugriff: 2.11.2023]
- Watchlist Internet (2023c): Vorsicht vor Abnehm-Pillen: Bestellen Sie nicht bei diaetolin.com. 2023, URL: <https://www.watchlist-internet.at/news/vorsicht-vor-abnehm-pillen-bestellen-sie-nicht-bei-diaetolincom/> [Zugriff: 21.12.2023]