SINBAD

Sicherheit und Prävention vor organisiertem Internet-Bestellbetrug für Anwender durch Maßnahmen der Digitalen-Forensik

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIRAS Kooperative F&E-Projekte 2019	**Status**	abgeschlossen
Projektstart	01.10.2020	**Projektende**	30.09.2022
Zeitraum	2020 - 2022	**Projektlaufzeit**	24 Monate
Keywords	Internetbetrug; Bestellbetrug; Machine Learning; Digitale Forensik		

Projektbeschreibung

Internetbestellbetrug hat laut Lagebericht des Bundesministeriums für Inneres im Jahr 2019 einen historischen Höchststand erreicht (+32,3%) – bei der österreichischen Meldestelle Watchlist Internet gingen in diesem Zeitraum über 10.500 Meldungen von KonsumentInnen zu Abofallen, Markenfälschern und Fake-Shops ein. Der Faktor Preis und optimierte Wege der Kundenansprache wie Werbung auf Social Media nehmen eine entscheidende Rolle ein, darüber hinaus erschweren gewiefte Tricks, wie die Errichtung unterschiedlicher Landing Sites, die Rechtsdurchsetzung für Betroffene.
Prävention ist ein Schlüsselinstrument im Kampf gegen Internetkriminalität. Doch die Meldungen von KonsumentInnen erfolgen zeitverzögert, sind unvollständig und oft ist der Schaden entstanden, bevor ein Fake-Shop durch die ExpertInnen erfasst wurde. Technische Lösungen, die KonsumentInnen aktiv warnen und schützen gelten als eine wichtige Ergänzung zu Präventionsmaßnahmen. Diesbezügliche Machine Learning (ML) Verfahren zeigen in den letzten fünf Jahren zunehmend Erfolge. In Österreich ermöglicht das laufende Flaggschiffprojekt MAL2, die Klassifizierung von Fake-Shops mit Detektionsraten von über 90%. Ein überdurchschnittlich hoher Grad der Clusterbildung bei der Datenanalyse lässt die Hypothese zu, dass Fake-Shop Baukastensysteme im Einsatz sind und es sich teils um organisierte Kriminalität handelt; ebenfalls gibt es Hinweise auf Geldwäsche durch Fake-Shops. Aktuelle Forschungsansätze reichen nicht aus, um diesen Verdachtsmomenten nachzugehen, denn sie setzen auf flache ML-Modellen aufgrund einer unzureichenden Datenbasis.

Ausgehend davon leitet SINBAD einen konkreten Bedarf der Sicherheitsforschung in den Bereichen: Lücken des Informationsraums erschließen, benötigte Verbesserungen umsetzen, KonsumentInnen proaktiv schützen, Gegennarrative entwickeln, ab. Eine ¬umfassende Analyse von Fake-Shop-Betrugsmaschen erfolgt über (1) eine technikgestützte Erhebung mit Echtpersonen zu gelisteten Produkte und Preisen, (2) eine Dark-¬Web Recherche zu Fake-Shop-Baukastensystemen, (3) eine Untersuchung der Zielgruppenadressierung (Werbung, Social Media, Suchmaschinen) betrügerischer Angebote und Bedürfniserhebung von KonsumentInnen.

Aufbauend auf existierenden MAL2 Ergebnissen realisiert SINBAD ein Multi-Task ML System zur Detektion von Fake-Shops, das autonom entscheidet, wann Parameter in der Entscheidungsfindung zu berücksichtigen sind. Durch ein proaktives Screening von neu registrierten Domains der DACH Region wird die Effizienz des Fake-Shop-AI-Detektor Prototypen zur

Senkung des Window of Opportunity (WoO) betrügerischer Angebote evaluiert und ein interdisziplinärer Maßnahmenkatalog abgeleitet.

Das Ziel des Projektes ist es durch innovative user-zentrierte Erhebungsmethoden, datengestützte Modelle und Vertiefung der Machine Learning Verfahren neue Erkenntnisse zur proaktiven Fake-Shop Detektion zu gewinnen und wirkungsvolle Gegennarrative unter Einbindung des Bedarfsträgers BMASGPK für die Verwertung der Ergebnisse im Stakeholder-Dialog aus Politik, Verbraucherschutz und E-Commerce zu entwickeln, mit denen KonsumentInnen gestärkt und geschützt werden.

Abstract

Based on the situation report of the Federal Ministry of the Interior, eCommerce fraud reached an all-time high in 2019 (+ 32.3%) - over 10,500 reports from consumers were received by the Austrian agency Watchlist Internet during this period including illegitimate subscription services, counterfeit goods and fake-shops. Factors such as the price or advertisements on social media play a decisive role in specifically addressing customers, and clever tricks such as customized landing-pages make enforcement of those affected difficult.
Prevention is a key instrument in fighting cybercrime. However, consumers hold back on reporting incidents, information reaches the experts in fragments and most often harm has already occurred before fake-shops are flagged. Technological solutions that actively warn and protect consumers are an important addition to preventive measures. Machine learning (ML) methods in this field have increasingly improved in the past five years. In Austria, the ongoing flagship project MAL2 enables the classification of fake shops with detection rates of over 90%. Data analysis presents an above-average degree of cluster formations - this leads to the hypothesis of the existence and usage of modular fake shop systems and partially organized crime; there are also indications of money laundering by fake shops. The limits of current research approaches to investigate these suspicions are defined by the use of shallow ML models due to insufficient data. The models lack robustness with regard to reliability and the small number of potentially available intrinsic features to explain the cluster formations, as well as their decrease in accuracy over time.

Based on this, SINBAD derives the specific need for security research in the following areas: exploring gaps in the information space; providing specific advancements; proactively protecting consumers and developing counter-narratives. A comprehensive analysis of fake shop fraud is carried out via (1) a technology-based monitoring with real persons for collecting data on listed products and prices, (2) a dark web research on modular fake shop systems, (3) analysis of ways and methods of group targeting by fraudulent eCommerce (advertising, social media, search engines) as well as assessing consumer needs. Building on existing MAL2 results, SINBAD is implementing a multi-task ML system for the detection of fake shops that autonomously decides when parameters must be taken into account in the decision-making process. By proactively screening newly registered domains in the DACH region, the efficiency of the fake shop AI detector prototypes in terms of its ability in decreasing the window of opportunity (WoO) of fraudulent offers is evaluated and an interdisciplinary catalog of measures is derived.
The goals of the project are to gain new insights into means of proactively detecting fake shops through user-centered methods, data-based models and the deepening of machine learning processes; to develop effective counter-narratives - under the involvement of the stakeholder BMASGPK which are based on the exploitation of key project results and through stakeholder dialogue with members of politics, consumer protection and e-commerce – through which consumers are strengthened and protected.

Projektkoordinator

- Österreichisches Institut für angewandte Telekommunikation

Projektpartner

- AIT Austrian Institute of Technology GmbH
- Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz
- Ciuvo GmbH
- X-Net Services GmbH