Bild: Rudolf A. Blaha

Affiliate-Eldorado

Partnerprogramm-Abzocke mittels Browser-Erweiterungen

Hunderttausende Euro Provision zahlen Online-Händler ihren Partnern jeden Monat aus – als Belohnung für generierte Einkäufe. Eine Recherche von c't legt nahe, dass sich dieses System technisch missbrauchen lässt, um Geldströme umzuleiten.

Von Holger Bleich und Herbert Braun

„Specialized in Data-Driven Lead Generation" sei sie, erklärt die Covus-Group auf ihrer Homepage. Der Minikonzern residiert in Berlin Mitte, beste Lage, Schwedter Straße 263, nahe Schönhauser Allee. CEO Sven Lubek hatte Covus 2003 gegründet und 2012 zu „Covus Venture" erweitert. Das operative Geschäft der Gruppe leitet der umtriebige Markus Malti, seit 2011 bei Covus und zuvor unter anderem „Senior Director of Strategy" bei der RTL Media Group.

Bei Covus war Malti umgehend aktiv geworden: Er hatte die Freemium GmbH aus der Taufe gehoben. Sie hat ihren Sitz in Sichtweite der Konzernzentrale von Covus, in der Schwedter Straße 9A. Ziel des Start-ups sei es, „qualitativ hochwertige, anwenderorientierte Software kostenfrei anzubieten. Durch Einbindung optionaler Partnerangebote und Featuresales auf Micropayment-Basis erfolgt die Monetarisierung", so erklärte man damals. Freemium pushte seine Tools, beispielsweise die „Free System Utilities", die „Windows von unnötigem Ballast befreien" sollten, in diverse Download-Portale.

Die gepriesene „Monetarisierung" kam allerdings weniger gut an: Bei den Portalen häuften sich Nutzerbeschwerden, weil offenbar lästige und eventuell gefährliche Werbe-Programme von Freemium mitinstalliert wurden. Die Tools flogen reihenweise aus den Verzeichnissen, beispielsweise aus denen von Computer Bild und Chip. Schlimmer noch: Antiviren-Portale veröffentlichten Anleitungen, wie die Freemium-GmbH-Malware zu entfernen sei. Avira, ein Produzent von Antiviren-Software, ließ 2015 sogar gerichtlich feststellen, dass seine Tools Freemiums Software als „potenziell unerwünschte Anwendungen" (PUAs) deklarieren dürfen.

Kleine Brutkasten-Welt

Um potenziell unerwünschte Anwendungen könnte es nun anderswo in der Unternehmensgruppe gehen. Szenenwechsel, wenige Meter weiter: In Obhut ihres Inkubators Covus werkelt auch die Wonderize GmbH. Sie firmiert unter derselben Berliner Adresse wie der Mutterkonzern. Diese Tochter hieß noch bis Mitte 2017 Cassius Media GmbH und hat mehrere Wechsel in der Geschäftsführung hinter sich. Aktuell führt Stefanie Peckmann die Firma, vormals COO bei der Freemium GmbH. Prokura hatte ausweislich des Handelsregisters bis April 2017 Freemium-Chef Malti – die Welt ist klein im Brutkasten.

Wonderize betreibt im Wesentlichen das Portal gutscheincodes.de. Dort werden mit allerlei bunten Bannern Rabattaktionen von Online-Shops beworben. Mal ein Acht-Euro-Bonus für Neukunden, mal das 150-Euro-Versprechen bei Neueröffnung des Girokontos. Wenn ein Nutzer auf eines der Banner klickt und letztendlich auf den beworbenen Deal eingeht, verdient Wonderize mit. Das Stichwort lautet Affiliate-Marketing.

Wonderize ist ein großer Player im Partnerprogramm-Business. Worum geht es da? Ein Website-Betreiber, beispielsweise ein Blogger, wirbt für Shops, die etwas verkaufen wollen – und verdient am Verkauf nach festgelegten Sätzen mit. Das wohl größte Partnerprogramm, oder im Fachsprech Affiliate-Marketing-Programm, stellt derzeit Amazon bereit: Ein Blogger bespricht ein Buch positiv und setzt einen Partner-Link zu Amazon.de darunter. Klickt der Blog-Leser den Link und kauft anschließend das Buch, erhält der Blogger als „Affiliate" eine Vermittlerprovision – und kann damit beispielsweise die Kosten für den Betrieb seines Blogs decken.

Tolle Sache, könnte man meinen: Der Händler verkauft mehr, und der Werbetreibende ist motiviert, weil er von jedem Sale etwas abbekommt. Eine echte Win-Win-Situation. Weil das – meist unbemerkt vom Kunden – schon so lange so gut ineinandergreift, haben sich Vermittler herausgebildet, die sich zwischen die Werbenden und die Händler schalten, die Affiliate-Netzwerke. Diese Unternehmen stellen Partnerprogramm-Infrastruktur bereit und zwacken im Gegenzug bei jedem Deal als Mittler eine Provision ab.

Knackpunkt in diesem System ist die Tracking-Technik. Um eine Provision zuzuordnen, muss der Händler wissen, über welchen Weg sein Käufer zu ihm in den Webshop gelangt ist. Bei „Pay-per-Sale"-Provisionierung (PPS) geschieht das meist über Cookies oder mit der Übergabe einer eindeutigen Partner-ID in der URL, mit welcher der Affiliate auf den Händler verlinkt. Letzteres klappt nur, wenn sich der Weiterleitung direkt der Kauf anschließt.

Die meisten Partnerprogramm-Betreiber setzen bevorzugt auf das „Last-Cookie-Wins"-Prinzip: Kommt der potenzielle Kunde über einen Affiliate, wird ein Cookie in den Browser gesetzt, in das die ID dieses Partners geschrieben ist. Kauft der Kunde erst einmal nichts, kommt aber später über einen anderen Partner wieder zurück, wird diese ID durch die des aktuellen Partners ersetzt. Kauft der Kunde nun etwas, wird die Provision dieser aktuellen ID zugewiesen. Der Händler belohnt hier also den Partner, der zuletzt den Besucher auf die Ziel-Seite weitergeleitet und zu einem Abschluss gebracht hat.

Dubiose Software

Große Partnerprogramm-Anbieter und Handelskonzerne zahlen monatlich hundertausende Euro an teilnehmende Affiliates aus. Es geht hier also um sehr viel Geld. Dem gegenüber sind die eingesetzten Tracking-Techniken erschreckend schlecht gegen Missbrauch gesichert. Das entscheidende Manipulationsinstrument liegt in der Hand des Kunden – es ist sein Web-Browser. Gelänge es, Schad-Software in Form von Add-ons in den Browser zu implantieren, wäre es möglich, unbemerkt vom Kunden Referrer zu manipulieren, Cookies umzuschreiben und damit in großem Stil Geldströme umzulenken – ein Schreckensszenario für das Affiliate-Business.

Es gibt unseren Recherchen zufolge Grund zur Annahme, dass genau dieses Szenario längst Wirklichkeit ist. Im Mittelpunkt der von uns beobachteten Aktivitäten stehen Unternehmen der Berliner Covus-Gruppe sowie ein dubioser thailändischer Software-Hersteller, der angeblich in einem Vorort von Bangkok ansässig ist und eine ganze Reihe deutschsprachiger Add-ons für Firefox und Chrome auf den Markt geworfen hat.

Add-ons der „Saphire Max Media Co Ltd" fanden sich bis vor kurzem in den Stores von Mozilla und Google, aber auch auf diversen Homepages, die immer in ähnlichem Template-Design gestaltet waren. Sie hießen beispielsweise Great Dealz, Offers Olymp, Lotta Deals oder Wallet Protector. Laut der immer gleichen Beschreibung sollten sie „aktuelle Rabatte, Gutscheine und Aktionen deiner Lieblings-Online-Shops direkt im Browser" anzeigen, was sie gelegentlich tatsächlich auch taten.

Auch die Homepage zu einem Add-on namens LuckyDealz passt genau in dieses Schema. Die Domain lucky-dealz.de ist wie die der Saphire Max Media von „Mohamed Yosadi" aus dem ägyptischen Kairo registriert. Allerdings: Im Impressum findet man nicht Saphire Max Media, sondern jene Cassius Media GmbH, die in das erwähnte Covus-Unternehmen Wonderize überging. Gibt es einen Zusammenhang zwischen Wonderize und den Add-ons?

Add-on-generierte Provisionen

Einige der Add-ons werden in Antiviren-Foren immer mal wieder als Malware deklariert. Wir haben uns beispielhaft aktuelle Versionen der beiden Saphire-Add-ons Great Dealz für Chrome und Wallet Protector für Firefox heruntergeladen. Anschließend haben wir ihren Code analysiert und mitgeschnitten, was sie treiben, während der Nutzer surft. Einen ausführlichen Bericht dazu lesen Sie auf Seite 26.

Zusammengefasst: Die beiden Add-ons wurden aktiv, wenn im Browser ein Webshop aufgerufen wurde, bei dem Wonderize entweder direkt oder über ein Affiliate-Netzwerk als Partner registriert ist. Unseren Beobachtungen zufolge sendeten sie je nach Tracking-Verfahren entweder unbemerkt vom Nutzer via URL-Referrer eine Affiliate-ID oder hinterließen sie im Provisions-Cookie des Shops. In beiden Fällen ging es stets um Affiliate-Accounts von gutscheincodes.de, dem Portal von Wonderize.

Dieses verdeckte Verhalten der Add-ons sorgte dafür, dass für jeden Kauf des Browser-Nutzers in diesem Shop eine Provision generiert wurde – allerdings ohne dass er über ein Banner auf gutscheincodes.de bewusst dorthin gelangt wäre.

Gigantische Abzocke?

Wie hoch der so zustande gekommene Umsatz von Wonderize sein könnte, erschließt sich mit einem genaueren Blick auf das Affiliate-Portfolio von gutscheincodes.de: Wonderize hat augenscheinlich das Who-is-who der Affiliate-Anbieter im Programm. Mit otto.de ist der zweitstärkste deutsche Webshop ebenso vertreten wie MediaMarkt, opodo, verivox, comdirect, 1&1 oder innogy. Wer fehlt, ist Amazon. Dazu muss man wissen, dass Amazon.de für seine gut funktionierende Betrugserkennung bekannt und in der Branche durchaus respektiert ist.

heise Investigativ

Viele der c't-Investigativ-Recherchen sind nur möglich dank Informationen, die Leser und Hinweisgeber direkt oder anonym an uns übermitteln.

Wenn Sie selbst Kenntnis von einem Missstand haben, von dem die Öffentlichkeit erfahren sollte, können Sie uns einen anonymen Hinweis oder brisantes Material zukommen lassen. Nutzen Sie dafür bitte unseren anonymen und sicheren Briefkasten.

https://heise.de/investigativ

Der Download-Manager von Computer Bild fordert dazu auf, das schädliche Add-on Great Dealz mit zu installieren.

Ausweislich des Geschäftsberichts hat Wonderize seine Bilanzsumme von 2015 (838.039 Euro) zu 2016 (1.692.689 Euro) glatt verdoppelt. Der Bericht für 2017 liegt noch nicht vor. Webtraffic-Analyse-Dienste wie Similarweb liefern allerdings interessante Zahlen: Seit Mitte 2017 sind demnach die Site-Besuche auf gutscheincodes.de explodiert. Im Dezember 2017 hat Similarweb 1,29 Millionen Abrufe gezählt – ein Plus von knapp 26 Prozent allein gegenüber dem Vormonat und eine Vervielfachung gegenüber August 2017.

Was Similarweb allerdings auch bestätigt: Den massiven Zuwachs hat gutscheincodes.de nicht echten Website-Besuchern zu verdanken, sondern Weiterleitungen aus der Amazon-Cloud. Im Dezember 2017 erfolgten demzufolge gerade mal zwei Prozent der Abrufe direkt über URL-Eingaben in den Web-Browser, rund 94 Prozent dagegen über Referrals. Nahezu alle dieser Referral-Zugriffe kamen von einem einzigen Host, nämlich einer Instanz von CloudFront, dem Content Delivery Network von Amazon. Gemäß unserer Analyse auf Seite 26 fungiert genau dieser Host als Proxy zwischen den Add-ons Great Dealz sowie Wallet Protector und gutscheincodes.de.

Kombiniert man die stark anschwellende Traffic-Statistik aus 2017 mit der Bilanzsumme des Jahres 2016, und geht man außerdem realistisch von einer Affiliate-Provision pro Kauf zwischen 5 und 10 Prozent aus, ergeben sich stattliche Summen. Sollten sich unsere Beobachtungen bestätigen, hätte Wonderize wohl jeden Monat mehrere hunderttausend Euro an Provisionen von den Add-ons in die Kasse gespült bekommen.

Helfershelfer

Doch eine solche Masche müsste doch den Partnerprogramm-Anbietern auffallen? Um sicherzugehen, dass wir richtig liegen, weihten wir einen großen deutschen Online-Händler, der seinen Namen hier nicht genannt sehen möchte, in unsere Recherche ein. Nach einigen Tagen eigener technischer Analyse bestätigte ein Sprecher des Konzerns verwundert unsere Beobachtungen. Der Sprecher kündigte Konsequenzen an. Man erwäge, eine Strafanzeige zu stellen sowie Schadensersatzansprüche auf dem zivilrechtlichen Weg geltend zu machen.

Erstaunlich ist der Verbreitungsgrad der Add-ons: Zum Beispiel Great Dealz: Mitte Januar 2018 verzeichnete der Chrome-Add-on-Store allein für diese Erweiterung knapp 100.000 Installationen – Ende Oktober 2017 waren es noch 77.500. Es bleibt die Frage, auf welchen Wegen die Add-ons auf Nutzer-Rechner gelangen. Nach unseren Beobachtungen machen sich an dieser Stelle „Synergie-Effekte“ in der Covus-Gruppe im wahrsten Sinne des Wortes bezahlt. Hier kommt die zu Beginn dieses Artikels erwähnte Freemium GmbH von Markus Malti ins Spiel.

Diese Firma macht Geschäfte mit einem großen Download-Portal: Der Software-Service von computerbild.de läuft teilweise über einen sogenannten „Download-Manager“. Falls ein Nutzer tatsächlich einmal die Nutzungsbedingungen in Gänze durchliest, bekommt er unter Punkt 6.1 zu sehen: „Der COMPUTER BILD-Download-Manager wird in Kooperation mit der Freemium GmbH, Schwedter Straße 9a, 10119 Berlin (nachfolgend Freemium) zur Verfügung gestellt.“

Freemium agiert hier als sogenanntes Bundling-Netzwerk. Der Kunde lädt nicht direkt gewünschte Software, sondern einen Installer herunter. Vor der Installation der Software versucht dieses Programm, den Kunden zu überreden, noch dieses oder jenes Tool mitzuinstallieren. Und tatsächlich fanden sich in unseren Tests auffällig oft Add-ons von Saphire Max Media darunter.

Möchte ein Nutzer das unerwünschte Add-on später wieder loswerden, öffnet sich ein weiterer Verbreitungsweg: Die Deinstallation nervt mit Hinweisen auf andere Add-ons von Saphire Max Media. Gut möglich, das einige Nutzer hier direkt vom Regen in die Traufe geleitet wurden.

Plötzlich Funkstille

Eine Kooperation zwischen Saphir Max Media und Wonderize lässt sich nicht beweisen. Wir konfrontierten sowohl Saphire als auch Wonderize und Freemium mit unseren Beobachtungen und baten um Erklärungen. Trotz jeweils zweimaliger Anfrage und Fristverlängerung erhielten wir von den beiden Berliner Unternehmen keine Antworten. Allerdings beobachteten wir kurz nach unseren ersten Anfragen vom 2. Februar 2018 interessante Änderungen.

Viele Add-ons von Saphire Max Media verschwanden aus den Stores der Browser-Hersteller. Der erwähnte CloudFront-Server lieferte einigen installierten Add-ons keine Referrer-URLs mit Affilliate-IDs von gutscheincodes.de mehr. Kurze Zeit drauf waren auch die Websites zu den Add-ons nicht mehr abrufbar. Die von uns zuvor sezierten Add-on-Versionen (siehe Seite 26) änderten ihr Verhalten. Selbstverständlich hatten wir zuvor jeden unserer Schritte präzise dokumentiert.

Sollte sich unser Verdacht bestätigen, läge hier wohl ein groß angelegter, gewerbsmäßiger Betrug vor. Geschädigt wären sowohl die Händler als auch alle Blogger, YouTuber und Website-Betreiber, denen die Saphire-Erweiterungen Provisionen vor der Nase weggeschnappt hätte. Und für die Add-on-Nutzer bliebe das mulmige Gefühl, Software installiert zu haben, die hinterrücks Daten auf dem Rechner manipuliert. *(hob@ct.de)* c't