Die geheimen Chats der Netzbetrüger

Mit gefälschten Inseraten erbeuten sie jedes Jahr Millionen Euro – gerade vor Weihnachten tappen gutgläubige Internetkäufer in ihre Falle. Die SZ hat erstmals Nachrichten von Nutzern des „Crimenetwork“ ausgewertet

VON HANNES MUNZINGER, LEA WEINMANN UND NILS WISCHMEYER

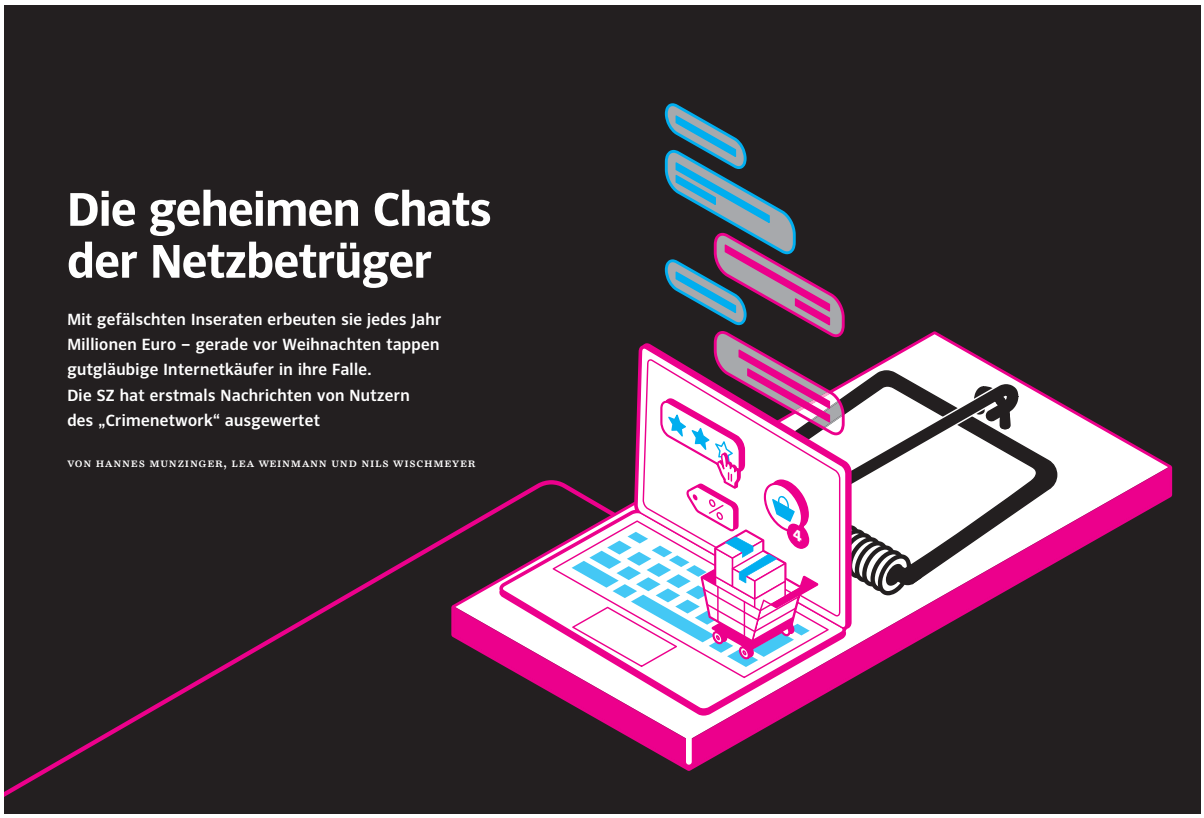


ILLUSTRATION: CAROLINE VOGT

Vielleicht findet man ja noch was bei Ebay-Kleinanzeigen. Kurz vor Weihnachten ist die Plattform die letzte große Hoffnung vieler Menschen, die noch nach einem Geschenk suchen. Manche wollen nicht mehr viel Geld ausgeben, andere können es schlicht nicht. Und bei Ebay-Kleinanzeigen oder auf abseitigen Onlineshops geht es oft ein bisschen günstiger. Doch die Schnäppchenjagd kann gefährlich werden. Denn während sich ahnungslose Geschenkesucher durch die Angebote kämmen, haben Internetbetrüger schon längst die Fallen für die Schnäppchenjäger aufgestellt. Und das läuft so wie hier zwischen den Nutzern mit den Pseudonymen *lockdownlothar* und *3komma3*:

lockdownlothar schätze mal du bist sway, oder?
3komma3 moin ja
lockdownlothar was kann ich für dich tun?
3komma3 würd gern testweise 10 inserate kaufen für klaz

„Klaz“ steht für Ebay-Kleinanzeigen, die Inserate sind Teil der Betrugsmasche.

lockdownlothar können wir gern machen
lockdownlothar Preissegment und sonstige Artikelwünsche?
3komma3 am besten nieschen
3komma3 preis ab 500

Die Nachrichten sind ein realer Ausschnitt aus dem Chat zwischen zwei mutmaßlichen Internetkriminellen. Einer von ihnen ist *3komma3* – oder *sway*. Er benutzt beide Pseudonyme auf Jabber, einem Instant-Messaging-Dienst, ähnlich wie früher MSN. Das Forum, über das sie sich kennen, ist das „Crimenetwork“, ein Marktplatz für Kriminelle, der quasi alles anbietet, was es auf dem legalen Markt nicht gibt: gefälschte Onlineshops mit erfundenen Produkten, geklaute Identitäten, gekaperte Bankkonten. Wer suchet, der findet.

In Internetforen finden die mutmaßlichen Betrüger alles, was sie für die Abzocke brauchen

Die ahnungslosen Shopper sehen nur Inserate mit Schnäppchen und können nicht widerstehen. Sie klicken, bezahlen – und gehen leer aus. Das Produkt kommt nie an, das Geld läuft auf ein von den Betrügern gekapertes Konto und ist weg. Die Täter brauchen dafür nicht mehr als einen Computer und eine ordentliche Portion kriminelle Energie. Jedes Jahr erschwindeln sie auf diese Weise Millionen Euro.

Im Jahr 2020 wollten die Ermittler dem kriminellen Forum einen harten Schlag verpassen, 1400 Beamte durchsuchten zahlreiche Gebäude. Ausgetrocknet haben sie das Netzwerk damit offensichtlich nicht. Denn einige Chatnachrichten haben *lockdownlothar* und *3komma3* erst Anfang dieses Jahres geschrieben.

Die Nachrichten zeigen: Die Menschen hinter den Pseudonymen arbeiten nicht in großen Banden, sie sind Einzeltäter. Jeder betrügt für sich. Aber sie tauschen sich aus, bieten einander Dienstleistungen an, manche werden auch richtig gute Kumpels. Mehr als 20 000 Nachrichten konnte die *Süddeutsche Zeitung* einsehen und deren Echtheit anhand einiger zugehöriger Bitcoin-Transaktionen stichprobenweise verifizieren. So kommt man den mutmaßlichen Betrügern ganz nah – bis hin zum gemeinsamen Chat.

sway hat zwischen Ende Januar und Anfang April 7300 Nachrichten geschrieben, mehr als alle anderen Personen, die in den Dateien auftauchen. Wie tickt jemand, der mutmaßlich Hunderttausende Euro mit Gaunerei von seinem Rechner zu Hause macht?

Seine normale „Arbeitszeit“ liegt offenbar zwischen elf und 22 Uhr, die meisten Nachrichten hat er in diesem Zeitraum geschrieben. Warum ausgerechnet von *sway* so viele Chats in der Datei gelandet sind, ist zunächst nicht klar. Möglich, dass er in der Szene sehr aktiv ist und ein großes Netzwerk hat. Auch möglich, dass ihm jemand eins auswischen wollte.

Sein Job in der Szene sei der eines „Shop filler“, schreibt *sway* einem seiner Chatpartner. Soll heißen, dass er wohl Fake Shops aufsetzt und seine Konten mit dem Geld der Leute füllt, die darauf hereinfallen. Die Chats zeigen, dass er offenbar zudem Menschen mit gefälschten Inseraten auf Ebay-Kleinanzeigen betrügt.

Täglich chattet *sway* mit Dienstleistern, die ihm viel seiner Arbeit abnehmen – und dabei ordentlich mitverdienen. In den Chats fragt *sway* ihre Leistungen an, feilscht um Preise, bemängelt schlechte Ware. Er kauft Dienstleistungen ein, um mutmaßlich selbst betrügen zu können. „Crime as a service“ nennt man dieses System. Mit 30 Pseudonymen hat *sway* in den gut drei Monaten geschrieben. Bei manchen scheint er Stammkunde zu sein, andere sind wohl eher Kumpels.

Ein Teil von *sways* Alltag besteht offenbar darin, potenzielle Opfer mit gefälschten Online-Inseraten bei Ebay-Kleinanzeigen anzulocken. Betrüger kopieren dafür in der Regel schon bestehende, echte Anzeigen und versuchen, diese auf der Plattform zu platzieren. Solche Fake-Inserate

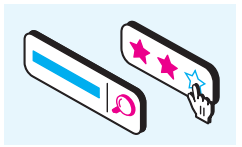
gibt es auch bei Amazon oder anderen Online-Marktplätzen. *sway* lässt sich diese Inserate – in den Chats schreibt er von „insis“ – von anderen basteln, etwa von *raes*:

3komma3 moin
3komma3 würd gern paar insis kaufen
3komma3 10x zum testen
raes nischenprodukte?
3komma3 jo
raes sind 80 dann, im angebot

Am Ende des Gesprächs kauft *sway* Inserate für 150 Euro. Damit eröffnet er sich die Chance, in einem Monat potenziell 35 Millionen Nutzer bei Ebay-Kleinanzeigen bestehlen zu können.

Und Ebay-Kleinanzeigen? Das Unternehmen kennt das Problem und trifft eigenen Angaben zufolge technische Vorkehrungen, beachtet auch Hinweise der Nutzer und warnt vor Auffälligkeiten. Ein Sprecher sagt, dass Kundinnen und Kunden besser nicht auf Vorkasse bestellen sollen und das man alles tue, um die Sicherheit der Kunden zu gewährleisten.

sway hat zu diesem Zeitpunkt 20 neue Inserate. Zur Bezahlung schickt er Geld an *raes*, natürlich nicht per Bankkonto, sondern per Bitcoin-Wallet. Das ist die digitale Geldbörse, die man braucht, um Kryptowährungen wie Bitcoins zu versenden und zu empfangen. Sämtliche Transaktionen, die je mit Bitcoin getätigt wurden, sind in der Blockchain hinterlegt und mittels einfacher Online-Tools für jeden öffentlich einsehbar. Und tatsächlich dokumentiert die Blockchain einige Stunden nach *sways* Nachricht eine Transaktion von umgerechnet etwa 150 Euro.



Besonders Nischenprodukte sind gefragt. Experten sagen, dass Menschen vor allem dann in die Falle tappen, wenn ein Produkt gerade knapp ist und wenn Käufer bereit sind, dafür in Vorkasse zu gehen. Das kann die neue Playstation ebenso sein wie Brennholz. Der mutmaßliche Verbrechensdienstleister hat Rudergeräte als „Geheimtipp“ empfohlen, die gingen gerade „wie Gold“. Logisch, in Zeiten der Pandemie wollen die Menschen zu Hause Sport treiben. Die Frage, welche Produkte besonders „gut gehen“, treibt *sway* sowieso regelmäßig um. Öfter wird gefachsimpelt:

serkan36 bruder
serkan36 ich brauch einfach junky zeug zum inserieren
3komma3 was ist junky zeug
serkan36 so dj scheiß unn gitarren
serkan36 da rasten die leute aus
3komma3 oke bro
3komma3 SAU VIEL INSERIEREN
3komma3 attacke ok
serkan36 ja ich brauch aber halt auch inserate die ballern
serkan36 un keine einbauküchen unn rasenmäher traktoren
serkan36 hol mir plattenspieler unn so djay scheißdreck

In den Chats geht es außerdem um: Hanteln, Pferdesattel, Kettensägen, Elektrorollerl. Die mutmaßlichen Gangster scannen permanent den Markt – und stellen entsprechend ihre Fallen. Gerade während der Vorweihnachtszeit ist für Internetbetrüger Hochkonjunktur: „Je mehr Leute online shoppen, desto mehr tappen auch in die Fake-Shop-Falle“, warnt Iwona Husemann von der Verbraucherzentrale NRW. Wegen der 2-G-Regel im Einzelhandel würden dieses Jahr wohl besonders viele aufs Onlineshopping ausweichen, vermutet sie. Hinzu kämen Lieferengpässe bei Spielwaren und Elektronik – noch ein Grund mehr, sich nach anderen Angeboten umzuschauen.

Neben gefälschten Inseraten bei Ebay versucht *sway* offenbar, Verbraucher mit Fake Shops hinters Licht zu führen. Statt einzelner falscher Anzeigen schaltet *sway* dafür gleich eine ganze Website, die wie ein seriöser Onlineshop mit zahlreichen Produkten wirken soll. Nichts auf diesen Seiten existiert tatsächlich. Für sein aktuelles Fake-Shop-Projekt beauftragt *sway* einen anderen Chatpartner, bei „Crimenetwork“ nennt er sich *simonerus*. Sein Auftrag: die Inhalte von den Seiten seriöser Online-Versandhändler kopieren und für die Fake Shops nachbauen. Die beiden arbeiten schon seit einigen Tagen zusammen. Währenddessen kommen sie ins Plaudern, über Bitcoin und die Gewinne, die sie mit dem Onlinebetrug erzielen:

sway zu viel geld ausgegeben letzte zeit
simonerus haha. was hast du dir noch zugelegt
sway puh paar autos
simonerus wie machst so viel geld ohne was zu machen
sway gut ich leb von dem vor monaten verdienten noch haha
simonerus was war das denn 20 30k
sway nene. war schon gut
simonerus ich habe 700 gemacht etwa. letztes jahr
sway dann haste echt hohe ausgaben
simonerus dieses jahr will ich 1mio erreichen. egal wie
simonerus dann erstmal pause

Kurz darauf schreibt *sway*, dass er im vergangenen Jahr zwischen 100 000 und 200 000 Euro verdient habe. Ob das stimmt, kann die SZ nicht prüfen. Doch die Summen, die er laut den Bitcoin-Transaktionen überweist, lassen vermuten, dass es bei seinen Geschäften tatsächlich um viel Geld geht.

Laut Ermittlern sind die wenigsten Onlinebetrüger professionelle Programmierer oder gar Hacker. Wozu auch die Mühe? Für Onlinebetrug finden sich Schritt-für-Schritt-Anleitungen in Foren wie dem „Crimenetwork“. Dort geht es ums Geschäft und um Persönliches. Einer schreibt, er habe als Kind Pokemon-Karten gestohlen, ein anderer arbeitet nicht, wenn die Freundin dabei ist. Und manchmal kriegen sie auch Gewissensbisse, einer schreibt: „Feiern kann man sich darauf nicht, ehrlich gesagt. Zumal man auch immer Angst haben muss, dass man morgens unschön geweckt werden könnte.“ Was er meint: von der Polizei.

Für *sway* alias *3komma3* steht derweil offenbar der nächste Schritt an. Denn beißt ein Opfer bei Ebay-Kleinanzeigen oder einem seiner Fake Shops an, braucht er eine Rechnung, damit der Handel möglichst echt aussieht. Für den Dienstleister *bigfootcnw* eine schnelle Angelegenheit:

3komma3 moin
3komma3 kannste mir schnell ne rechnung für ne kaffeemaschine basteln
bigfootcnw hi
bigfootcnw bist du sway ?
3komma3 jop
3komma3 die maschine ises
3komma3 schaffstes vllt in 5 min
bigfootcnw ich bin gerade dabei

So fälschen mutmaßliche Cyberkriminelle wie *sway* wohl auch Fotos von Personalausweisen und Paketmarken. *sway* kauft eine solche beispielsweise bei *Whit3CNW* und schreibt: „Brauche ne 100% TID grad geht das schnell.“ TID, noch so eine Abkürzung. Sie steht für Transaktions-ID, die Sendungsnummer, mit der man den Sendestatus von Paketen verfolgen kann. Sie ist mit einer falschen Identität gekauft. Abschicken wird *sway* sein imaginäres Paket wohl nie, aber mit der realen Sendungsnummer kann er seine Opfer länger hinhalten.

Was *sway* zum Abkassieren seiner Opfer noch fehlt, ist ein Bankkonto, denn sein eigenes kann er nicht benutzen. Im „Crimenetwork“ kauft er sich vermutlich deshalb einen sogenannten Bankdrop, ein Konto, das zuvor jemand ergaunert hat. Besonders häufig kommen in den Chats gekaperte Konten von Onlinebanken wie N26, Fidor oder der Postbank vor. Viel seltener, aber deshalb begehrter und teurer scheinen hingegen Konten der Sparkasse und der Consorsbank zu sein.

Geklaute Bankkonten sind ein wichtiges Puzzleteil in diesem Betrug. Dass es sie überhaupt gibt, liegt an der Naivität der Menschen. Sie surfen im Internet und sehen dort eine gut getarnte Anzeige der Betrüger: „Tester für Kontoeröffnung gesucht.“ Die Ahnungslosen klicken darauf und eröffnen tatsächlich ein Konto bei einer Bank. Dafür erhalten sie von den Betrügern etwas Geld – quasi als kleine Belohnung. Im Anschluss erzählen die Betrüger den Menschen, dass sie ihnen die Zugangsdaten geben sollen. Sie würden das Konto dann schließen. Das aber ist, wie die ganze Test-Aktion, eine Lüge. In dem Moment, in dem die Menschen ihre Daten weitergeben, können die Betrüger das legal eröffnete Konto als ihres ausgeben. Wenn bei Ebay-Kleinanzeigen der Käufer nun Geld überweist, landet es auf diesem gekaperten Konto und fließt von dort aus ab. Spuren zu den eigentlichen Tätern hinterlässt das nicht, stattdessen gerät der ahnungslose Testkunde ins Visier.

Wenn die Polizei die Opfer kontaktiert, ist es oft zu spät und die Täter sind über alle Berge

Auf Anfrage teilten alle Banken mit, dass sie sich des Problems bewusst sind und es durch die Pandemie zugenommen habe. Sie würden aktiv dagegen vorgehen, sowohl mit technischen Lösungen als auch durch Aufklärung. Ganz zu verhindern seien betrügerische Eröffnungen aber nicht, solange Menschen auf die Maschen der Betrüger hereinfallen, so der Konsens.

Wenn die Polizei bei den Opfern klingelt, ist es meist zu spät. Weil alles anonym und schnell läuft, ist es für die Ermittler schwer, den Betrügern auf die Schliche zu kommen. Für Verbraucher ist das keine gute Nachricht. Sie sind quasi hilflos und begegnen vielleicht eines Tages einem mutmaßlichen Betrüger wie *sway*. In den Chats taucht seine Telefonnummer auf. Als die SZ ihn anruft, nimmt er nicht ab. Im Messenger Telegram antwortet er. Zu den Vorwürfen will er sich zunächst nicht äußern und schreibt, dass es sich „wohl um einen Irrtum“ handele. Auf eine ausführliche Anfrage schickt er Links zu den Social-Media-Profilen der SZ-Autorin und der -Autoren, sagt, damit könne man einiges anfangen und dass man sich eine Veröffentlichung gut überlegen solle. Es ist seine vorerst letzte Nachricht.