Plötzlich schrieb er auf Kyrillisch: Wie Betrüger Tutti missbrauchen

Mehrere hundert Personen wurden allein im Dezember mit einer ausgefeilten Betrugsmasche auf dem Online-Marktplatz konfrontiert. Auch unser Autor wurde angeschrieben. Dann verrieten sich die Cyberkriminellen.

Illustration: Oliver Marx

Christopher Gilb

Einem Gegenstand, den man nicht mehr benötigt, ein zweites Leben zu schenken und dafür auch noch etwas Geld zu erhalten: Das ist das Konzept des Online-Marktplatzes Tutti. Auch der Autor dieser Zeilen schaltete dort kürzlich ein Inserat für ein Bücherregal auf. Um es Interessenten zu ermöglichen, ihn flexibel zu kontaktieren, liess er es zu, dass seine Handynummer angezeigt wird. Nur wenige Sekunden später erhielt er schon eine erste Anfrage per Whatsapp, gefolgt von einer zweiten. Ob das Produkt noch zu verkaufen sei, wollte der erste Interessent wissen. «Klar», schreibt der Autor zurück. Auf dem Anzeigebild ist ein Mann mit seiner Familie zu sehen. Ob das Regal irgendwelche Schäden habe, will der potenzielle Käufer wissen. Eine berechtigte Frage, denkt sich der Autor, und schickt ein Foto eines kleinen Kratzers zurück.

Als Antwort erscheint ein Daumen nach oben und die Bestätigung, dass er es kaufen wolle. Das ging aber schnell. Doch dann schreibt der potenzielle Käufer, dass er das Möbelstück nicht wie gewohnt abholen könne, und fragt, ob die Lieferung über das Onlineangebot der Post erfolgen könne. Auf der Post-Website könne der Verkäufer seine Zahlungsdaten angeben, nach ausgeführter Bezahlung werde die Lieferung dann über eine Spedition durchgeführt. Das macht den Autor stutzig, vor allem auch, weil ihm auffällt, dass beide Nummern, von denen ihm geschrieben wurde, eine ausländische Vorwahl haben, bei der einen Estland und bei der anderen Grossbritannien. Und auch die diversen Grammatikfehler stechen ihm jetzt ins Auge. Er will lieber kein Risiko eingehen und beschliesst, die Nummern zu blockieren.

Masche ist bekannt als «Tokenized Fraud»

Wie Recherchen zeigen, handelt es sich um eine bekannte Masche, die «Tokenized Fraud» genannt wird. Auf Cybercrimepolice.ch, einem Angebot der Kantonspolizei Zürich, wird sie beschrieben: Die Betrüger versuchen, ihre Opfer auf eine gefälschte personalisierte Post-Website zu locken. Dort finden sich Informationen zur angebotenen Ware und dem vereinbarten Kaufpreis plus die Angaben einer Lieferadresse, welche allerdings frei erfunden ist. Klickt das Opfer dann auf den Knopf «Fortfahren», wird es zur Eingabe der Kreditkartendaten aufgefordert. Diese wollen die Täter kopieren, dabei spricht man auch von «Phishing». Verfügen sie dann darüber, wird auch noch die 2-Faktor-Authentisierung ausgehebelt, indem der Verkäufer aufgefordert wird, die Push-Nachricht der Bank-App zu bestätigen. So können die Täter dann mit der auf ihrem Handy virtualisierten Kreditkarte über Bezahldienste wie Google Pay oder Apple Pay auf Kosten des Opfers einkaufen gehen.

317 Personen haben über Cybercrimepolice.ch angegeben, von dieser Masche betroffen zu sein. Tutti teilt mit, allein im Dezember 360 Rückmeldungen zur besagten Betrugsmasche erhalten zu haben, von insgesamt 1300 Betrugsmeldungen im gleichen Zeitraum. Erst kürzlich habe man die Bemühungen im Kampf gegen Betrug durch den Einsatz neuer, spezifischer Schutzsoftware ausgedehnt, um jede Art von Betrug so effektiv wie möglich zu verhindern, schreibt eine Sprecherin. Aber: «Gegen solche Kontaktaufnahmen und Chatverläufe über SMS oder Whatsapp können wir leider nichts unternehmen, da diese ausserhalb unseres Systems verschickt werden.»

Doch was ist über die Täter und ihr Vorgehen bekannt? Die Kantonspolizei Zürich schreibt auf Anfrage, dass die Betrüger erfahrungsgemäss eine Web-Applikation nutzen würden, weshalb die Rufnummer nur einmal für die Verifizierung benötigt werde und allenfalls nicht mal im Besitz der Betrüger sein muss; deshalb auch die Nummern mit der ausländischen Vorwahl. Konkrete Angaben zur Herkunft der Täter kann die Polizei nicht machen, nur dass es sich in der Regel nicht um Einzeltäter handelt.

Der Autor beschliesst, diesen auf den Zahn zu fühlen. Und deblockiert den zweiten «Interessenten», mit dem er bisher noch nicht geschrieben hat. Wieder läuft der Chat gleich ab, doch dieser will noch wissen, ob das Produkt aus Naturholz sei. Eine passende Frage für ein Bücherregal. Kurz darauf kommt der Link zur angeblichen Post-Website. Nur dass zwar oben «*www.post.ch*» erscheint und auch das Bild darauf hindeutet, der Link aber zu einer Website «post-ch…» führt.

Die Maschine als Komplize des Menschen

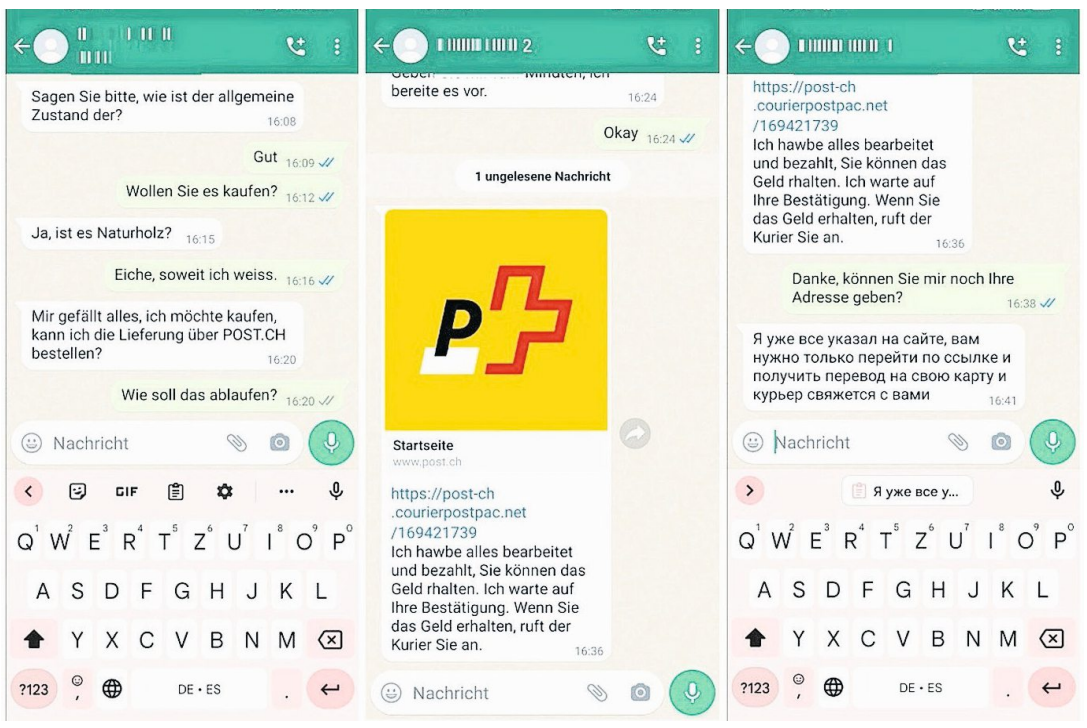
Statt auf den Link zu klicken, schickt ihm der Autor eine Nachfrage und will die Zustelladresse wissen. Und da verrät sich der Betrüger, denn zurück kommt eine Antwort auf Kyrillisch. Auf Nachfrage löscht er sie schnell und schickt die deutsche Übersetzung, mit der Entschuldigung, dass er einen Übersetzer verwendet. Der Autor fragt ihn darauf, ob er aus Russland stamme. Er schreibt: Weissrussland. Ob der Versand dann kein Problem sei? «Ich bin in Lausanne», schreibt er schnell. Der Autor versucht, die Person anzurufen, doch es kommt nur eine automatische Antwort, dass der Inhaber der Nummer nicht zu erreichen sei. Ab diesem Moment ist auch der Chat tot und Nachrichten werden nicht mehr gelesen. Die Spur verliert sich.

Eine Frage lässt den Autor nicht los. Wie kann es sein, dass die Betrüger im gleichen Moment, in dem ein Angebot aufgeschaltet wird, schon den Verkäufer kontaktieren können? Sind da etwa Chatbots, also automatische Dialogsysteme, im Spiel, die nach dem immer gleichen Schema automatisch Daten abfischen? Die Kantonspolizei Zürich schreibt, es sei auffällig, dass mehrere Betroffene angegeben hätten, dass sie bereits kurz nach Aufschaltung ihrer Inserate von den Betrügern kontaktiert worden seien. Doch der Betrüger fragte ihn doch, ob es sich um Naturholz handle, eine individuelle Nachfrage, die wiederum für einen Menschen sprechen würde, denkt sich der Autor.

Sophie Hundertmark von der Hochschule Luzern ist Expertin im Bereich der Chatbots und setzt mit Hilfe von Chatbot-Tools auch selbst solche um. Ihr ist es wichtig zu betonen, dass in diesem Fall nicht Chatbots für den Betrug verantwortlich sind, sondern Betrüger, die allfällige Sicherheitslücken von Plattformen geschickt auszunutzen wissen. Sie glaubt, dass es sich beim Betrug um eine Mischung von Chatbots und Mensch handelt. Vermutlich werde zuerst ein Web-Crawler eingesetzt, also ein Computerprogramm, das automatisch Websites nach gewissen Vorgaben absucht, etwa neu aufgeschalteten Inseraten mit angegebener Handynummer.

Die Verkäufer werden dann mit einer automatisierten Nachricht kontaktiert. Die Nachfrage zum Naturholz, glaubt sie, könne von einem Chatbot stammen. Dieser könne etwa für jede Inseratekategorie mit fünf Standardfragen ausgestattet sein. Das verringere die Gefahr, dass Anbietenden gleichartiger Artikel dieselbe Nachfrage gestellt wird. «Und die Chance, dass etwa die Frage nach dem Naturholz auf ein Möbel zutrifft, ist relativ hoch.»

Zum Einsatz komme ein Mensch erst dann, wenn das Schema durchbrochen wird; etwa durch den Autor, der nicht direkt auf den Link geklickt hat, sondern eine unerwartete Nachfrage gestellt hat. Also dann, als dem vermeintlichen Chatpartner der erste Fehler unterlief, da er vergass, die Antwort zu übersetzen.



Auszüge aus dem Chat mit dem vermeintlichen Käufer. Bild: Screenshot Christopher Gilb

> «Die Chance, dass etwa die Frage nach dem Naturholz auf ein Möbel zutrifft, ist relativ hoch.»

Sophie Hundertmark
Expertin für Chatbots HSLU

Das rät «Tutti» den Inserenten

— Telefonnummer in Inseraten ausblenden, einzig das Kontaktformular von Tutti für den Austausch nutzen.

— Nie auf solche Anfragen eingehen, die Telefonnummer blockieren und sich mit dem Kundendienst von Tutti in Verbindung setzen.

— Auf keine Links klicken. Sollte bereits ein Link geöffnet worden sein, niemals Kreditkartendaten preisgeben.

— Sollten Nutzerinnen und Nutzer bereits in die Falle getappt sein, umgehend die Bank kontaktieren und/oder die Kreditkarte sperren. *(chm)*