Schwarzmarkt Deutschland

Der Handel mit Drogen, Waffen und Kreditkartendaten im deutschen Cyber-Untergrund

Auf deutschsprachigen Online-Markplätzen herrscht ein offener Handel mit Waffen, Falschgeld, Ausweisdokumenten, Kreditkartendaten und Drogen. Trojaner-Entwickler und Betrüger bieten ihre Dienste gegen Entgelt an. Nachdem die Geschäfte jahrelang weitgehend unbehelligt über die Bühne gingen, herrscht nun Aufruhr in der Szene: Der Polizei ist ein Schlag gegen den wohl bekanntesten Drogenmarkt gelungen und der zentrale Drahtzieher eines anderen Portals hat sich mutmaßlich abgesetzt.

Von Uli Ries

Es wird gedealt, was geht, in den dunklen Ecken des Internets. Neben Hehlerwaren gehen auch gefälschte Ausweise, Kreditkartendaten, Waffen und Drogen über den virtuellen Ladentisch. Zudem werden allerlei zwielichtige Dienstleistungen angeboten. Im deutschsprachigen Raum waren zwei der prominentesten Umschlagplätze für Illegales der Drogenshop Chemical Love und das Untergrundforum crimenetwork.biz (CNW). Beide verschwanden im Mai 2016 quasi gleichzeitig aus dem Netz. Im Fall von Chemical Love sind die Gründe klar: Razzien der Polizei, bei denen fünf Nutzer von Chemical Love festgenommen und 54 Kilogramm Amphetamin, gut vier Kilogramm Heroin, rund 1,3 Kilogramm Kokain sowie etwa 25 000 Ecstasy-Tabletten beschlagnahmt wurden. Gerüchten aus der Szene zufolge soll das jedoch nur ein Teil dessen gewesen sein, was Chemical Love verkaufte.

Noch laufen die Auswertungen der Vernehmungen sowie der in den Niederlanden und Bulgarien sichergestellten Datenträger der Server. Daher entzieht es sich der Kenntnis von Markus Heusler, Staatsanwalt bei der zuständigen Staatsanwaltschaft Verden, „ob sich einer der Festgenommenen dazu bekannt hat, auch Betreiber der Seite gewesen zu sein." Der Zugriff gelang, nachdem die Ermittler erfuhren, „dass drei mutmaßliche Haupttäter anlässlich einer Drogenlieferung in einem Lager zusammentreffen werden, so dass dies ein guter Zeitpunkt für einen Zugriff war." Gut 1500 Drogendeals mit einem Gesamtvolumen von 1,3 Millionen Euro sollen laut den Ermittlern innerhalb eines Jahres abgewickelt worden sein. Ein Administrator eines Szeneforums behauptet jedoch, dass diese Zahl viel zu niedrig angesetzt sei.

Ob auch das Verschwinden des wahrscheinlich größten deutschsprachigen Untergrundforums crimenetwork.biz mit diesem Zugriff zusammenhängt, können weder Staatsanwalt Heusler noch einer der beteiligten Ermittler der Polizei bestätigen. Wahrscheinlich im Jahr 2006 gestartet, hatte CNW kurz vor dem Verschwinden gut 84 000 registrierte Nutzer, die über vier Millionen Posts verteilt auf gut 190 000 Threads verfasst haben. Zu erreichen war CNW, genau wie Chemical Love, sowohl über das Tor-Netzwerk als auch über das offene Web.

Bitcoins im Mixer

Nach allem, was über die jeweiligen Administratoren „sync" von CNW und „z100" von Chemical Love bekannt ist, arbeiteten sie eng zusammen und nutzten wahrscheinlich sogar die gleiche Serverinfrastruktur. Angeblich flossen rund 10 000 Euro monatlich an sync für dessen Dienste. Eventuell war die Ausschaltung des den Ermittlern ebenfalls bekannten CNW also nur ein Kollateralschaden des Schlags gegen Chemical Love.

Denkbar ist allerdings auch, dass sich sync abgesetzt hat. Möglicherweise, weil die Luft nach der Razzia und den Verhaftungen im Fall von Chemical Love dünner wurde. Oder um sich das ihm anvertraute Geld unter den Nagel zu reißen. Eine in der Szene kursierende Vermutung stützt sich unter anderem darauf, dass offenbar ein sync in seiner Funktion als Treuhänder zuzuordnendes Bitcoin-Wallet am 10. Mai abgeräumt wurde. Der Gegenwert von gut 33 500 US-Dollar wurde wahrscheinlich an einen sogenannten Bitcoin-Mixer transferiert. Die kommen zum Einsatz, um Zahlungsströme im recht transparenten Bitcoin-Netz zu verschleiern. Gerüchten zufolge soll

In Untergrund-Foren werden gefälschte Ausweise auf Wunschnamen angeboten.

der transferierte Betrag nur ein Bruchteil dessen gewesen sein, worüber sync verfügte.

Einblicke

Ein Experte von Trend Micro, der sich umfassend mit der Szene befasst hat, erklärte gegenüber c't, dass der hiesige Untergrund erheblich übersichtlicher sei als beispielsweise der russische. Gegenüber den übrigen europäischen Online-Treffpunkten lägen die deutschsprachigen Foren und Marktplätze in Sachen Nutzerzahlen und Transaktionen jedoch vorn. Der Forscher möchte nicht namentlich genannt werden. Er hat seine Erkenntnisse in einem umfangreichen Bericht zusammengefasst.

Ein Grund für die Popularität könnte nach Einschätzung des Forschers schlicht die Tatsache sein, dass nicht jeder angehende Online-Ganove der englischen oder gar russischen Sprache mächtig ist. Zudem schneidern die Anbieter ihre Waren und Dienste auf hiesige Bedingungen zu: So stammen die angebotenen Login-Daten oftmals von deutschen Opfern. Und zum Anliefern der mit geklauten Daten gekauften Waren dienen keine Privatanschriften von angeworbenen, meist ahnungslosen Zeitgenossen, sondern die beliebten Packstationen von DHL.

Der Fachmann hat bei seiner Analyse etwa knapp zehn Foren und zwei Marktplätze ausgemacht, die hauptsächlich von deutschsprachigen Nutzern frequentiert werden. Er konzentrierte sich im Rahmen seiner Auswertung auf die vier nach Nutzerzahlen größten Foren und einen großen Marktplatz. Gut 20 000 aktive Teilnehmer und ein Vielfaches an stummen Teilnehmern zählt der Forschungsbericht auf; einige hundert eindeutige Nicknames tauchen in identischer Schreibweise auch auf ausländischen Betrugsplattformen auf. Viele der Nutzer verwenden Avatarfotos, auf denen Kreditkarten, Drogen oder einfach große Mengen Bargeld zu sehen sind, was die Motivation der jeweiligen Forumsteilnahme unterstreichen dürfte.

Auf den Marktplätzen gehen die Transaktionen schnell und unbürokratisch über die Bühne, da keine Kommunikation zwischen Verkäufer und Käufer nötig ist. In den Foren lassen sich hingegen auch speziellere Angebote wie beispielsweise Bullet-Proof-Hosting in einem bestimmten IP-Bereich oder nach Kundenwunsch programmierte Skripte für Phishing-Attacken kaufen. Auch finden sich detaillierte Anleitungen, wie man am besten mit geklauten Kreditkarten bei Versandhändlern wie Zalando einkauft. Schenkt man den – oftmals dick aufgetragenen – Schilderungen Glauben, sind Bestellungen in Höhe von 2000 Euro machbar.

crimenetwork.biz: Illegales in Hülle und Fülle

Die Untersuchung des Trend-Micro-Forschers vermittelt auch einen Eindruck vom illegalen Treiben in dem gerade dahingeschiedenen crimenetwork.biz. Demnach lehnte sich das Angebot eng an die großen ausländischen Untergrundforen an. Neben den üblichen Diskussionsthreads gab es zahlreiche Unterforen, in denen Waren und Dienste feilgeboten wurden. Dort fand sich alles, was das Ganovenherz begehrt: Hehlerwaren, Falschgeld, verschreibungspflichtige Medikamente, Bahntickets und gefälschte Ausweise auf Wunschnamen. Auch digitale Güter wurden gehandelt: etwa Zugangsdaten für Online-Banking oder diverse bekannte Online-Händler.

Wer eine Stufe früher in der Nahrungskette stehen wollte, konnte zum Beispiel den auf Passwortklau spezialisierten Trojaner Triple CCC im Crimenetwork erwerben. Ebenfalls im Angebot war die Software Cube Recovery, mit der man beliebige Daten von infizierten Rechnern abgreifen kann.

Auf dem Marktplatz von crimenetwork.biz wurden unter anderem Hehlerwaren, Drogen, Waffen, Kreditkartendaten und Accounts für diverse Websites gehandelt.

Der deutschsprachige Entwickler verlangte eine „Spende“ in Höhe von mindestens drei Euro für den Download. Der Nutzer Statine programmierte Malware und Skripte zum Datenklau nach Maß. Diverse Nutzer lobten die Qualität seiner Arbeit. Dass Statine den Trend-Micro-Report kannte, zeigte der Footer, den er nach Erscheinen des Reports unter jedes seiner Postings packte: Er zitiert den Teil des Berichts, der sich auf ihn bezieht.

Auffällig war das Verquicken von herkömmlichen Cybercrime-Angeboten mit dem Verkauf von Drogen. Auf crimenetwork.biz fanden sich Banner und diverse weitere Links zu chemical-love.cc. Im russischen Untergrund seien dem Fachmann zufolge Foren für Drogen und Waffen meist getrennt von herkömmlichen Cybercrime-Plattformen.

So verdienen die Betreiber

Nachdem das Hosting der Seiten Geld und die Moderation zumindest Zeit kostet, müssen die Betreiber irgendwie am Treiben mitverdienen. Um möglichst viele Nutzer anzulocken, sind die Foren offen per Google aufzufinden. Auch das Registrierungsformular ist meist für jedermann zugänglich. Auch im Untergrund gilt die Faustregel: Mehr Nutzer, mehr Umsatz.

Der gängigste Weg zum Geldverdienen sind sogenannte Escrow-Services (Treuhänderdienste), wie sie nur in Foren, nicht aber auf den Marktplätzen angeboten werden: Foren-Administratoren wie sync fungieren als Mittler zwischen Käufer und Verkäufer. Sie nehmen vom Käufer die Zahlung und vom Verkäufer die – meist digital übermittelte – Ware entgegen und geben nach erfolgter Zahlung die Transaktion frei. Zwischen drei und 15 Prozent der Summe behalten die Treuhänder für sich, erklärt der Experte gegenüber c't. Üblicherweise wird mit Bitcoins gezahlt, oft werden auch Gutscheine oder Geschenkkarten für Online-Shops akzeptiert. All diese Zahlungswege sollen die Anonymität der Parteien sicherstellen. Im Fall des Crimenetwork-Forums dürfte dieses Treuhänder-Geld nun verschwunden sein. Online-Postings zufolge hat sync schon seit Anfang Mai keine ihm anvertrauten Beträge mehr ausgezahlt.

Wie viel die Betreiber mit ihren Diensten einnehmen, ist nicht bekannt. Aber bei besonders wertvollen Waren kann ein Treuhänder problemlos dreistellige Beträge als Provision einsacken. So kosten spezielle Kreditkarten bis zu 3500 Euro – etwa, wenn sie zu Unternehmen gehören. Die Verkäufer versprechen, dass die Karten hohe Verfügungslimits haben und einzelne betrügerische Transaktionen den Mitarbeitern des betroffenen Unternehmens nicht auffallen. Typischerweise dienen solche Karten in Firmen zum Buchen von Reisen: Sämtliche Flüge werden beispielsweise mit ein und derselben Kreditkarte bezahlt. Buchen nun die Online-Gauner mit eben dieser Karte Tickets für sich oder für Dritte, gehen diese Transaktionen wahrscheinlich unter. Die Chance, dass der Betrug auffliegt und die Karte gesperrt wird, ist eher gering.

Komplize Packstation

Eine Besonderheit des deutschen Online-Untergrunds ist das Angebot an Nutzerkonten für DHL-Packstationen. Zwar gibt es vergleichbare Paketaufbewahrungsmethoden auch in anderen Staaten. Wie der Forscher im Gespräch erklärte, würden aber nur hierzulande Packstationen zum Anliefern von heiklen Waren wie Drogen oder Waffen verwendet.

Die Preise für die meist per Phishing abgegriffenen Zugangsdaten der Packstation-Nutzer richten sich nach der Art des Kontos: Die 20 bis 25 Euro teuren Konten erlauben das vom Opfer unbemerkte Eintragen einer beliebigen Mobiltelefonnummer im Kundenprofil. Auf diese Weise kann der unerwünschte Mitnutzer kurz vor dem Abholen seiner Sendung („Droppen“) die zum Empfang notwendige mTAN an seine Nummer schicken lassen. Schon für fünf Euro gibt es Zugriff auf Konten, bei denen sich die Telefonnummer nur durch einen Anruf beim Kundendienst von DHL ändern lässt, was Aufwand und Risiko erhöht. Aber auch dafür gibt es eine Lösung: In den Foren tummeln sich Dienstleister, die Anrufe wie diese für die Betrüger übernehmen. Der Service lässt auch etwa damit beauftragen, telefonisch das Verfügungslimit einer geklauten Kreditkarte zu erhöhen. Die ebenfalls zum Abholen nötigen goldenen Karten gehen für sieben Euro über die Ladentheke. Sie müssen lediglich mit der Nummer der gewünschten Packstation beschrieben werden.

Wie groß der Anteil der betrügerischen Lieferungen an die insgesamt

Professional Social Engineering: Der Anrufservice lässt sich etwa damit beauftragen, den Verfügungsrahmen einer geklauten Kreditkarte zu erhöhen.

„DW Performance-Guns" verkauft umgebaute Schreckschuss-Waffen und Eigenentwicklungen.

acht Millionen Nutzer der Packstationen ist, konnte DHL auf Nachfrage nicht sagen: Man werde von Kunden nicht immer in Kenntnis gesetzt, wenn es zu unerwünschten Sendungen komme.

Im Visier der Strafverfolger

Das illegale Treiben im deutschen Cyber-Untergrund entgeht natürlich auch den deutschen Behörden nicht, wie der Fall Chemical Love zeigt. Dazu Markus Heusler von der Staatsanwaltschaft Verden: „Ermittlungen in deutschen Untergrundforen sind zwar nicht Tagesgeschäft, aber dennoch regelmäßig Bestandteil unserer Tätigkeiten. Auch im Moment haben wir weitere deutsche Foren im Blick." Auf einer Sicherheitskonferenz Anfang Juni zeigte sich der BKA-Vize Peter Henzler selbstbewusst: „Wir sind in der Lage, im Internet zu ermitteln, Akteure umzudrehen, ihre Plattformen zu übernehmen und Bitcoins sicherzustellen."

Offensichtlich wurde die Arbeit der Strafverfolger beispielsweise auch durch die Verhaftung eines 29-jährigen Drogenhändlers aus Sankt Augustin. Aller Wahrscheinlichkeit nach handelt es sich dabei um einen Händler, der unter dem Nickname Oxywhite unter anderem im Crimenetwork-Forum aktiv war. Die zuständige Staatsanwaltschaft ermittelt noch und kann daher nicht bestätigen, dass es sich bei dem nach der Durchsuchung Anfang Dezember 2015 Festgenommenen tatsächlich um Oxywhite handelt. Dafür spricht, dass dessen Online-Profile seit dieser Zeit stillliegen. Fest steht, dass es Verbindung zwischen einem Waffenhändler in Baden-Württemberg (DW Performance Guns) und einem Forennutzer namens Oxywhite gab. Der Waffenhändler stand im Verdacht, Schusswaffen an die Terroristen von Paris geliefert zu haben und stand daher unter Beobachtung. Oxywhite bestellte über eines der nur per Tor zugänglichen Foren eine halbautomatische Waffe bei DW Performance Guns. Nachdem die Behörden hinter dem Waffenlieferanten den verdächtigten Händler aus Baden-Württemberg vermuteten, geriet Oxywhite mit ins Visier der Fahnder.

Wenig überraschend dauerte es nach dem Verschwinden von crimenetwork.biz nicht lange, bis ein fast identisch aufgebautes Angebot auftauchte, um die ehemaligen Nutzer aufzufangen. Es ging am 16. Mai online, als Administrator fungiert mit Mr. White ein ehemaliger Moderator von CNW. Die Moderatoren sowie etliche der ersten angemeldeten Nutzer waren ebenfalls schon zu CNW-Zeiten aktiv. Einige Tage nach dem Start waren bereits gut 2700 Konten registriert.

Angriff auf heise.de

Das neue Forum passt offenbar auch in der Szene nicht jedem in den Kram: Nachdem wir Pfingsten auf heise.de über die neuen Entwicklungen berichtet hatten, beobachteten wir über Tage hinweg massive DDoS-Attacken gegen unsere Server. Der mutmaßliche Täter, offenbar ein Unterstützer eines anderen Untergrundforums, kontaktierte uns per Mail und forderte uns auf, die Meldung zu entfernen. Wir verstehen dies als Angriff auf die Pressefreiheit und sind der Aufforderung nicht nachgekommen. Die Angriffe hatten zur Folge, dass Teile der Seite immer wieder über mehrere Stunden nicht erreichbar waren.

Als Begründung nannte der Bekenner, das Forum sei eine Fälschung und man treibe mit solchen Meldungen Nutzer „in die Arme von Fakes". Über die Absurdität, dass ein Forum für Betrüger und Kriminelle statthafter sein soll als ein anderes, macht man sich in diesen Kreisen offenbar keine Gedanken.

Dass beim illegalen Waffenkauf auf dubiosen Internetseiten offenbar doch noch Hürden lauern, hat der ARD-Reporter Reinhold Beckmann in einer Mitte Mai ausgestrahlten Folge der Reportage-Reihe #BECKMANN gezeigt. Es gelang ihm zwar mithilfe eines Mittelsmanns, eine Kalaschnikow auf dem Marktplatz „Black Market" zu bestellen – geliefert wurde das mehrere hundert Euro teure Maschinengewehr jedoch nie. *(ct@ct.de)* c't