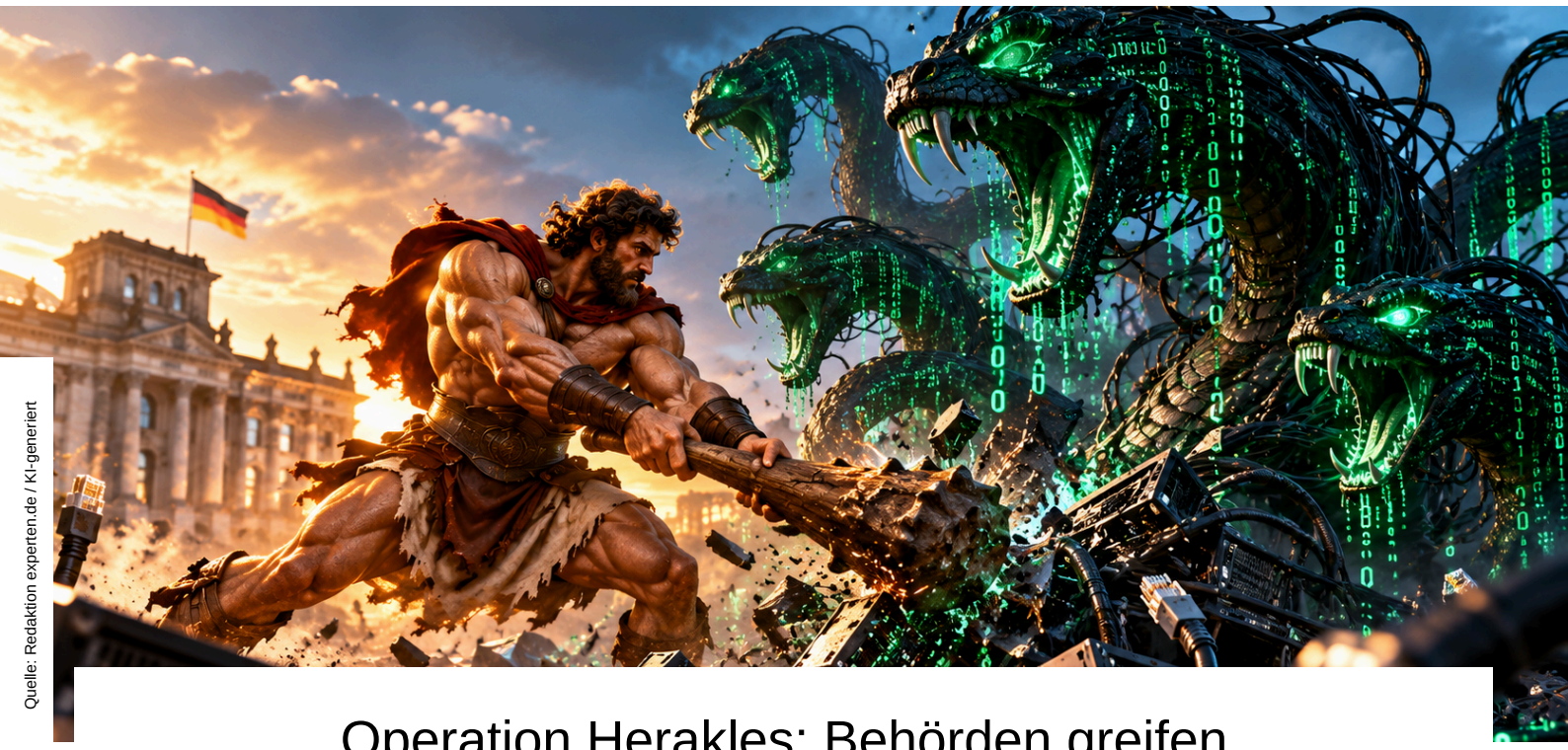
expertenReport



Quelle: Redaktion experten.de / KI-generiert

Operation Herakles: Behörden greifen Infrastruktur der Anlagebetrüger systematisch an

Michael Fiedler

Erst verschwanden Tausende betrügerische Trading-Websites, dann die zugehörigen Telefonnummern. Mit der „Operation Herakles“ gehen Ermittler und Aufsichtsbehörden inzwischen systematisch gegen die Infrastruktur des Cyber-Anlagebetrugs vor. Allein in den vergangenen drei Monaten wurden 9.304 deutsche Rufnummern abgeschaltet – und der Zugriff reicht inzwischen bis zu den Telekommunikationsunternehmen.

Wie weit dieser Ansatz inzwischen reicht, zeigt die jüngste Bilanz der „Operation Herakles“. Das Cybercrime-Zentrum Baden-Württemberg (CCZ) bei der Generalstaatsanwaltschaft Karlsruhe und das Landeskriminalamt Baden-Württemberg haben gemeinsam mit Bundeskriminalamt, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Bundesnetzagentur und dem österreichischen Bundeskriminalamt innerhalb der vergangenen drei Monate 9.304 deutsche Rufnummern identifiziert und abschalten lassen.

Seit Beginn der Operation wurden damit insgesamt 13.888 mutmaßlich für Betrugsstraftaten genutzte Rufnummern abgeschaltet. Davon entfallen 13.397 auf Deutschland und 491 auf Österreich. Im Mittelpunkt steht insbesondere der sogenannte Cyber-Trading-Fraud, bei dem Anleger über vermeintliche Handelsplattformen zu Investitionen verleitet werden.

Von betrügerischen Websites zu Tausenden Telefonnummern

Die aktuelle Aktion ist Teil einer länger angelegten Strategie. Bereits 2025 richtete sich die Operation Herakles massiv gegen die Online-Infrastruktur der Täter. Im Juni und Oktober vergangenen Jahres gelang es den Ermittlern, insgesamt mehr als 2.200 mutmaßlich für Cyberbetrug genutzte Domains vom Netz zu nehmen. Im Dezember folgte der nächste Schritt: Rund 3.500 verdächtige Rufnummern wurden abgeschaltet. Im Oktober 2025 berichtete experten.de über die Beteiligung der BaFin an einem internationalen Schlag gegen Cybertrading-Betrug. Damals standen insbesondere manipulierte Handelsplattformen im Mittelpunkt. Eine weitere Aktion zeigte anschließend, wie stark die verschiedenen Bestandteile der Betrugsinfrastruktur miteinander verzahnt sind. Mit der jüngsten Abschaltung Tausender Telefonnummern wird nun sichtbar, dass aus

einzelnen Zugriffen zunehmend ein dauerhaftes Vorgehen gegen die Infrastruktur entsteht.

Behörden wollen Betrugsbekämpfung skalieren

Dafür haben die beteiligten Behörden nach eigenen Angaben inzwischen feste Strukturen und Verfahrenswege geschaffen. Sie sollen es ermöglichen, erhebliche Mengen mutmaßlich für Straftaten genutzter Rufnummern systematisch zu identifizieren und abschalten zu lassen. Dabei greifen unterschiedliche Instrumente ineinander: strafprozessuale Ermittlungen, polizeirechtliche Maßnahmen, Finanzaufsicht und Telekommunikationsaufsicht.

Die Behörden sprechen ausdrücklich von einem neuen strategischen Ansatz. Mit Herakles werde erstmals gemeinsam das Ziel verfolgt, die kriminelle Infrastruktur „systematisch und nachhaltig zu schwächen“ und die Täter aus dem Bundesgebiet zu verdrängen. Gleichzeitig sollen laufende Straftaten aufgeklärt, Tatverdächtige identifiziert und weitere potenzielle Opfer geschützt werden.

Damit reagiert die Strafverfolgung auf ein grundlegendes Problem des Cyberbetrugs: Kriminelle Geschäftsmodelle lassen sich digital vervielfältigen. Wird eine Website gesperrt oder eine Telefonnummer abgeschaltet, können neue Strukturen vergleichsweise schnell aufgebaut werden. Die Gegenstrategie besteht deshalb zunehmend darin, nicht nur einzelne Erscheinungsformen zu beseitigen, sondern ihre massenhafte Bereitstellung zu erschweren.

Bundesnetzagentur nimmt Telekommunikationsanbieter in die Pflicht

Bemerkenswert ist dabei die Rolle der Bundesnetzagentur. Sie ließ nicht lediglich verdächtige Nummern abschalten, sondern ergriff nach eigenen Angaben auch aufsichtsrechtliche Maßnahmen gegen die verantwortlichen Telekommunikationsunternehmen. Diese wurden aufgefordert, ihre Registrierungsprozesse anzupassen. Außerdem sollen sie die Compliance-Kontrollen ihrer Vertriebspartner und Händler verstärken und diese genauer überprüfen. Ziel ist es, bereits die missbräuchliche Registrierung und Nutzung von Rufnummern zu erschweren. Damit setzt die Operation inzwischen früher in der Betrugskette an. Nicht erst der betrügerische Anruf soll unterbunden werden. Erschwert werden soll bereits der Zugang zu jener Telekommunikationsinfrastruktur, die solche Anrufe in großer Zahl ermöglicht.

BaFin liefert Daten zu verdächtigen Rufnummern

Eine weitere Schnittstelle liegt bei der Finanzaufsicht. Die BaFin ermittelt in eigener Zuständigkeit gegen unerlaubte Geschäfte im Bereich Cyber-Trading. Ihre Ermittlungsergebnisse haben nach Angaben der beteiligten Behörden wesentlich dazu beigetragen, zahlreiche verdächtige Telefonnummern zu identifizieren. Das verdeutlicht die Besonderheit des Cyber-Anlagebetrugs: Er verbindet klassische Betrugsdelikte mit unerlaubten Finanzgeschäften, digitaler Infrastruktur und grenzüberschreitend arbeitenden Tätergruppen. Entsprechend reicht die Bekämpfung inzwischen von Polizei und Staatsanwaltschaft über Finanz- und Telekommunikationsaufsicht bis zu ausländischen Ermittlungsbehörden.

Woran Anleger betrügerische Angebote erkennen können

Trotz des Vorgehens gegen die Infrastruktur bleibt der Schutz potenzieller Opfer entscheidend. Polizei, Cybercrime-Zentrum und BaFin raten dazu, Trading-Plattformen vor einer Einzahlung sorgfältig zu überprüfen und sich nicht zu schnellen Investitionsentscheidungen drängen zu lassen. Besondere Vorsicht ist geboten, wenn Anbieter Zugangsdaten zum Onlinebanking oder Depot verlangen. Auch Kopien von Ausweisdokumenten oder Zahlungskarten sollten nicht leichtfertig übermittelt werden. Die BaFin weist zudem darauf hin, dass Anbieter von Finanz- und Wertpapierdienstleistungen in Deutschland grundsätzlich eine Erlaubnis benötigen. Anleger können deshalb vor einer Investition überprüfen, ob ein Unternehmen entsprechend zugelassen ist. Die jüngste Bilanz von Herakles zeigt allerdings auch, warum individuelle Vorsicht allein das Problem kaum lösen kann. Wenn innerhalb von drei Monaten mehr als 9.000 mutmaßlich für Betrugszwecke eingesetzte Telefonnummern identifiziert werden, spricht das für eine Infrastruktur, die auf Masse ausgelegt ist. Die Antwort der Behörden folgt inzwischen derselben Logik: Cyber-Anlagebetrug skaliert – und zunehmend soll auch seine Bekämpfung skalierbar werden.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4952096/Operation-Herakles-Behoerden-greifen-Infrastruktur-der-Anlagebetrueger-systematisch-an/