Organisierte Kriminalität im Internet: **Europols Vorgehen gegen Cyberkriminalität**

Von seinem Sitz im niederländischen Den Haag aus unterstützt Europol die Mitgliedstaaten bei der Verhütung und Bekämpfung aller Formen von schwerer internationaler und organisierter Kriminalität, Terrorismus und Cyberkriminalität.

Zu den Hauptprioritäten der Agentur zählt, wie aus der jüngsten Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität in der Europäischen Union (EU-SOCTA) hervorgeht, die Bekämpfung der Cyberkriminalität. In der EU-SOCTA werden für das Gebiet der EU als Hauptbedrohungen durch Cyberkriminalität Cyberangriffe, Online-Betrugssysteme und (online begangene) sexuelle Ausbeutung von Kindern genannt.

| **Europol, Organisierte Kriminalität im Internet: Europols Vorgehen gegen Cyberkriminalität**

PDF Web | ISBN 978-92-9414-070-8 | DOI-10.2813/6436249 | QL-01-25-021-DE-N

© Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung, 2025

Diese Zusammenfassung wurde zu Informationszwecken übersetzt. Bitte beachten Sie, dass die englische Fassung als offizielles Referenzdokument gilt.

Nachdruck mit Quellenangabe gestattet.

Bei der Verwendung oder Reproduktion von Fotos oder sonstigem Material, das nicht dem Urheberrecht der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung unterliegt, muss die Zustimmung direkt bei den Rechteinhabern eingeholt werden.

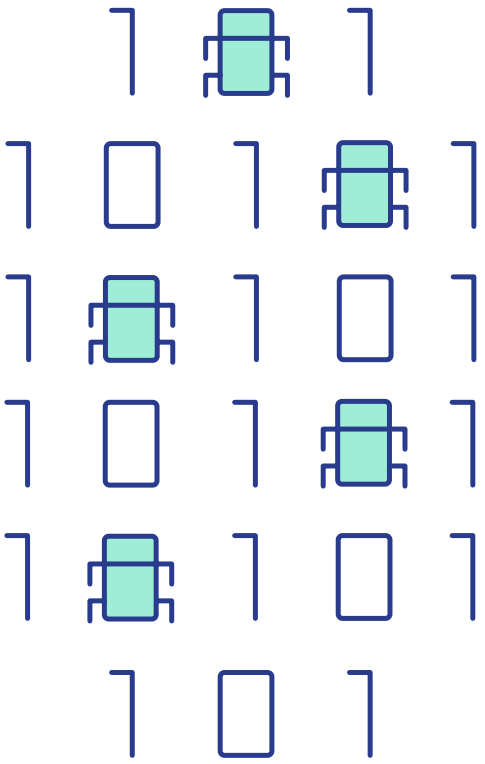
Zitation dieser Veröffentlichung: Europol, Organisierte Kriminalität im Internet: Europols Vorgehen gegen Cyberkriminalität - Zusammenfassung, Amt für Veröffentlichungen der Europäischen Union, Luxemburg, 2025.

Der vollständige Bericht ist auf der Europol-Website
www.europol.europa.eu

Cyberangriffe sind gezielte Online-Angriffe von Cyberkriminellen, die sich gegen kritische Infrastruktur, Regierungen, Unternehmen und Privatleute richten. Oftmals werden sie im Auftrag von Akteuren, von denen eine externe Bedrohung ausgeht, ausgeführt, wobei diese Akteure zunehmend staatsgetrieben und ideologisch motiviert sind.

Haupttrends bei Cyberangriffen:

- **Daten sind ein zentrales Handelsgut im Bereich der von Malware ausgehenden Bedrohung,** sei es als Mittel für die Tatbegehung, als Angriffsziel oder als bei Angriffen anfallendes Nebenprodukt.
- **Ermöglicht werden diese Straftaten durch die Crime-as-a-Service-Wirtschaft,** unter anderem durch Dark-Web-Marktforen für den Verkauf gestohlener Daten, durch Intrusion Services, aber auch durch kriminelle Hosting- und Proxy-Provider.
- **Der Bereich der Cyberkriminalität ist zunehmend fragmentiert:** Die Märkte und Ransomware-Gruppen existieren für immer kürzere Zeiträume und zersplittern immer mehr, was die Identifizierung der Akteure, von denen die Bedrohung ausgeht, erschwert.



Cybercrime-Netzwerke im Visier

Die Operation Eastwood richtete sich gegen das Cybercrime-Netzwerk NoName057(16). Diese interne Operation wurde vom 14. bis 17. Juli 2025 gemeinsam mit Eurojust durchgeführt.

Die für NoName057(16) handelnden Personen sind zumeist russischsprachige Sympathisanten, die mit automatisierten Tools digitale Überlastungsangriffe (sogenannte DDoS-Angriffe) ausführen. Sie agieren ohne förmliche Führung oder besondere technische Fähigkeiten und sind vor allem ideologisch motiviert und gewinngetrieben.

Die nationalen Behörden kontaktierten Hunderte Personen, die im Verdacht stehen, dieses Cybercrime-Netzwerk zu unterstützen. Über eine viel genutzte Messaging-Anwendung wurden diese über die behördlichen Maßnahmen informiert und darauf aufmerksam gemacht, dass ihre Handlungen nach nationalem Recht strafbar sind.

Mit der Operation wurde bislang erreicht, dass die aus 100 weltweit verteilten Computersystemen bestehende Infrastruktur für Angriffe gestört und ein erheblicher Teil der zentralen Server-Infrastruktur der Gruppe vom Netz genommen wurden.

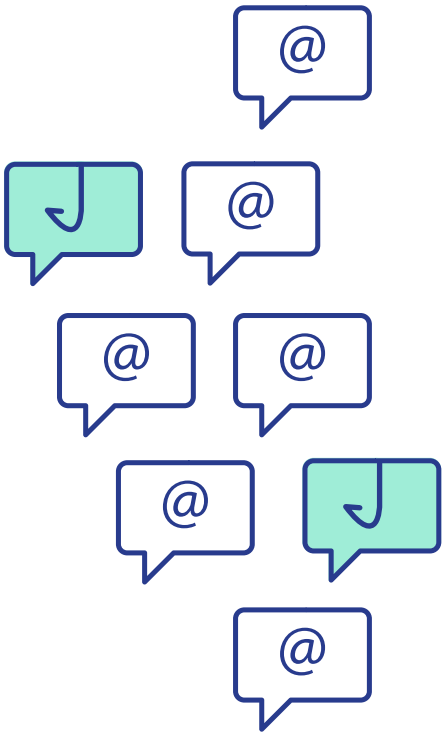
Der IOCTA-Bericht ist hier zu finden
↓

Online-Betrugssysteme sind einer der am schnellsten expandierenden Bereiche der organisierten Kriminalität, die sich gegen ein breites Spektrum von Opfern richtet. Der Onlinebetrug, der bereits ein enormes Ausmaß erreicht hat, dürfte, getrieben durch Fortschritte in den Bereichen Automation und KI, weiter zunehmen.

Haupttrends bei Online-Betrugssystemen:

- **Online-Betrugssysteme** sind immer schwerer aufzudecken, weil sie langfristig angelegt, maßgeschneidert und höchst kompliziert sind.
- **Große Sorge bereitet der Diebstahl personenbezogener Daten aus Zahlungssystemen.** Die Daten werden entweder direkt genutzt oder an andere Kriminelle verkauft, sodass die Opfer wiederholt Straftaten zum Opfer fallen.
- **Einige Betrüger sind technisch sehr versiert.** und in der Lage, ihre Methoden stets weiterzuentwickeln; wegen dieser Anpassungsfähigkeit der Angreifer dürften die Gefahren künftig noch größer werden.

Der Online-Betrugsszene ist ein sehr gut organisierter und hoch kompetenter Bereich der Kriminalität, der nicht nur Opfer ins Visier nimmt, sondern auch professionelle Dienstleistungen für Kriminelle anbietet. Die Betrüger wissen, sich fortschrittliche Technologien, menschliche Schwächen und Gesetzeslücken zunutze zu machen.



Ermittlungen gegen Phishing-as-a-Service-Plattformen

Bei der Zerschlagung von LabHost, einer der größten Phishing-as-a-Service-Plattformen der Welt, spielte Europol eine zentrale Rolle. Im Zuge der ein Jahr dauernden Operation fanden im Zeitraum 14. bis 17. April 2024 an insgesamt 70 Adressen weltweit Durchsuchungen statt, die zur Festnahme von 37 Verdächtigen führten.

Die Plattform LabHost bot im Monatsabonnement einen konfigurierbaren Service an, der von Phishing Kits bis zu Webseiten für Infrastruktur-Hosting-Angebote reichte. Je nach Abonnement wurde den Kriminellen Zugriff auf immer größere potenzielle Opfergruppen geboten, unter anderem auf Finanzinstitute, Postdienste und Anbieter von Telekommunikationsdiensten. Teil des Abos war ein Kampagnen-Tool namens LabRat, mit dem technisch unbedarfte Kriminelle die Angriffe in Echtzeit überwachen und steuern konnten.

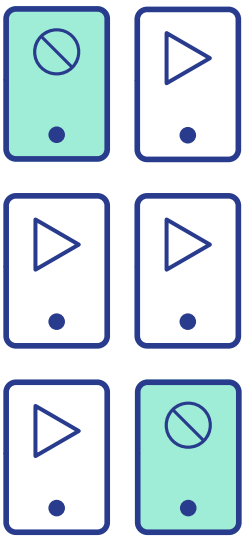
Durch diese Operation wurden bislang 40 000 Phishing-Domains und mehr als 10 000 Nutzer weltweit erkannt. Die von LabHost und LabRat erfassten Daten werden weiter für laufende internationale Operationen verwendet.

Höre dir unsere Podcast-Episode darüber an, wie Kriminalität online gefördert wird

(Online begangene) sexuelle Ausbeutung von Kindern bezeichnet den sexuellen Missbrauch von Personen unter 18 Jahren sowie die Erstellung und den Online-Austausch von Bildern solcher Missbrauchshandlungen. Dies ist eine besonders abscheuliche schwere Straftat, bei der Kinder körperliche und psychische Gewalt erleiden, die ihre Gesundheit und Entwicklung enorm beeinträchtigt.

Haupttrends im Bereich der sexuellen Ausbeutung von Kindern:

- **Im Zuge der digitalen Beschleunigung hat sich die online begangene sexuelle Ausbeutung von Kindern rapide weiterentwickelt.** Inzwischen gibt es grenzüberschreitende End-to-End-verschlüsselte Plattformen, auf der Straftäter nicht nur kinderpornografisches Material erstellen, speichern und austauschen, sondern auch Opfer kontaktieren und deren Vertrauen erschleichen können, um sich die Kinder gefügig zu machen.
- **Der Zugriff auf KI-Tools eröffnet neue Dimensionen der sexuellen Ausbeutung von Kindern.** Mit diesen Tools ist es möglich, bestehendes Material zu bearbeiten oder neuen Content zu erstellen, indem beispielsweise Erwachsenen ein jüngeres Aussehen gegeben wird oder aus harmlosen Bildern Nacktbilder gemacht werden.
- **Verschiedenste Gruppen, die digitale Plattformen für ihre Zwecke nutzen.** Weltweit werden digitale Plattformen dazu genutzt, Straftäter zu rekrutieren und Opfer zu finden, äußerste Grausamkeit zu normalisieren, Opfer zu erpressen, kinderpornografisches Material auszutauschen und sogar Personen zu radikalisieren, um sie für gewalttätigen Extremismus zu gewinnen.



Bekämpfung der sexuellen Ausbeutung von Kindern

Die Operation Stream (auch „Operation Kidflix“ genannt) ist eine der größten Operationen gegen die sexuelle Ausbeutung von Kindern in der Geschichte von Europol. Die 2022 begonnenen Ermittlungen führten schließlich zu den Aktionswochen im Zeitraum 10. bis 23. März 2025.

Die 2021 geschaffene Streaming-Plattform Kidflix erfreute sich unter Pädophilen schon bald großer Beliebtheit. Nach Behördenangaben wurden 91 000 verschiedene Videos mit einer Spielzeit von insgesamt 6 288 Stunden hochgeladen und geteilt. Anders als bei anderen Plattformen dieser Art konnten die Nutzer von Kidflix nicht nur kinderpornografisches Material herunterladen, sondern auch Videodateien streamen. Die Nutzer zahlten in Kryptowährungen.

Bislang wurden 1 393 Verdächtige ermittelt, 79 Verdächtige festgenommen, mehr als 3 000 elektronische Geräte beschlagnahmt; 39 Kinder konnten vor weiterem Missbrauch geschützt werden.

Nähere Informationen über Cyberangriffe, Online-Betrugssysteme und sexuelle Ausbeutung von Kindern sind in EU-SOCTA

Cyberkriminalität im Wandel: Datenverwertung

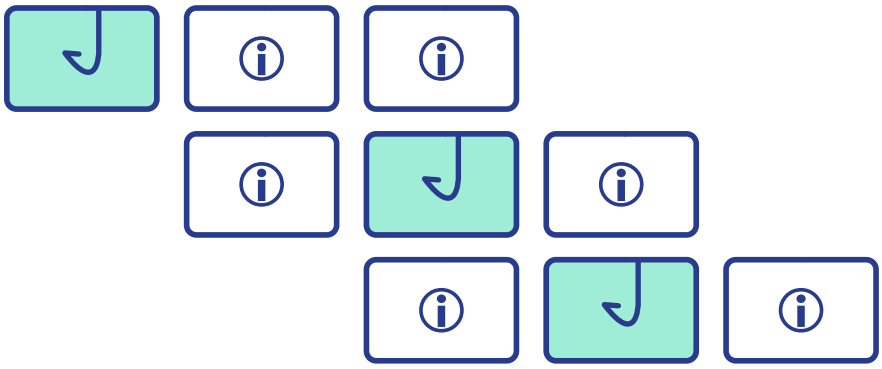
In den letzten zwölf Monaten hat Europol die von den neuen Trends in der Cyberkriminalität ausgehenden Bedrohungen weiter untersucht. Dabei kristallisierte sich heraus, dass der allgemeine Trend zum Datenmissbrauch die treibende Kraft hinter dem kriminellen Ökosystem ist, das von Onlinebetrug über Ransomware bis zu sexueller Ausbeutung von Kindern reicht. Dies war auch das zentrale Thema der dieses Jahr erschienenen Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet (Internet Organised Crime Threat Assessment, IOCTA) **Steal, deal, and repeat: How cybercriminals trade and exploit your data.**

„Gegen das, was man nicht versteht, kann man sich nicht verteidigen. Der von Europol vorgelegte Bericht IOCTA 2025 wirft ein Schlaglicht auf die Schattenwirtschaft, in der gestohlene Daten der Motor sind, der die gefährlichsten Cyberbedrohungen der heutigen Zeit vorantreibt. IOCTA 2025 liefert Strafverfolgern, Politik und Industrie die Informationen, die sie benötigen, um energisch dagegen vorzugehen."

Edvardas Šileris, Leiter des European Cybercrime Centre von Europol.

Dieses Jahr werden folgende Haupttrends hervorgehoben, an denen deutlich wird, wie Cyberkriminelle ihre Methoden anpassen und ihre Aktivitäten immer mehr ausweiten:

- **Von illegal erlangten Daten profitieren die verschiedensten Straftäter,** sei es, dass sie direkt aus den Daten Gewinn schlagen, sei es, dass sie sich die Daten zu anderen Zwecken verschaffen, etwa zur Begehung weiterer Straftaten.
- **Cyberkriminelle nutzen die verschiedensten Techniken, um sich Zugang zu personenbezogenen Daten zu verschaffen und diese zu stehlen,** wobei sie Schwachstellen der Systeme wie auch menschliche Schwächen geschickt zu nutzen wissen. Besonders häufig setzen sie auf Social Engineering.
- **Große Sprachmodelle (Large Language Models, LLMs) und andere Formen generativer künstlicher Intelligenz ermöglichen noch effektiveres Social Engineering** weil es damit möglich ist, die Kommunikation genau auf die Opfer zuzuschneiden und die strafbaren Handlungen zu automatisieren.
- **Ein Teil dieses kriminellen Ökosystems, in dem große Zuwächse zu verzeichnen sind, ist der Verkauf des Zugangs zu kompromittierten Systemen und Konten.** Zunehmend werden Dienste dieser Art wie auch damit zusammenhängende Leistungen von sogenannten Initial Access Brokern (IABs), d. h. von auf das Eindringen in fremde Netzwerke und Systeme spezialisierten Cyberkriminellen, auf speziellen kriminellen Plattformen angeboten, die wiederum von den verschiedensten Cyberkriminellen genutzt werden.
- **Data Broker sind auf vielen Plattformen aktiv, um ihre Machenschaften zu diversifizieren und ihre Resilienz gegen Strafverfolgungsmaßnahmen zu stärken.** Immer häufiger kommt es vor, dass auf Messenger-Diensten mit End-to-End-Verschlüsselung (E2EE) nicht nur für Geschäfte mit kompromittierten Daten geworben wird und derartige Geschäfte ausgehandelt und durchgeführt werden, sondern dass auch personenbezogene Daten der Opfer,unter denen sich auch Kinder befinden, weitergegeben werden.



Im Blickpunkt:
Angriffswege für die Datenernte

Cyberkriminelle setzen vielfältige Techniken ein, bei denen entweder Sicherheitslücken im System oder menschliche Schwächen ausgenutzt werden, um auf personenbezogene Daten zuzugreifen und diese zu stehlen. Immer häufiger werden Techniken des Social Engineering dazu eingesetzt, Daten zu erlangen, beispielsweise:

Phishing

Bei dieser Art von Angriff geht es darum, die Opfer mit Malware zu infizieren oder sie durch Täuschung dazu zu verleiten, ihre Passwörter auf Websites einzugeben, die vom Betrüger mittels Phishing Kits erstellt wurdens.

Infostealer

Diese Art Malware ist spezifisch darauf ausgelegt, sich illegal sensible Informationen aus kompromittierten Geräten zu verschaffen und so die Anmeldedaten, App-Tokens und Sitzungscookies zu erfassen. Dabei setzen die Straftäter mit Schadware-Anhängen/URLs versehene E-Mails, Textnachrichten oder Messages in sozialen Medien ein, um Malware in das System des Opfers einzuschleusen.

Vishing

Die Betrüger bringen die Opfer mit Telefonanrufen dazu, sensible Informationen preiszugeben; dabei nutzen die Täter Spoofing-Services[1] , die den Eindruck erwecken, dass es sich beim Anrufer um Personen oder Stellen handelt, die in der Gegend ansässig sind und einen guten Ruf genießen.

Botnetze zerschlagen

Operation Endgame ist Teil einer Serie von Operationen zur Zerschlagung von Botnetzen, die eine der größten Operationen ihrer Art ist. Sie begann im Mai 2024 und läuft weiterhin.

Botnetze sind Netzwerke, in denen mit Malware infizierte Geräte zusammengeschlossen sind und die von den Angreifern aus der Ferne und ohne Wissen der Gerätebesitzer gesteuert werden können. Für die Erstinfektion werden meist sogenannte Dropper oder Loader verwendet, eine Art Schadsoftware, die als „Türöffner“ dazu dient, weitere Malware in den Systemen zu installieren.

Unterstützt werden die laufenden Ermittlungen von Europol und der Gemeinsamen Taskforce gegen die Cyberkriminalität (J-CAT), die den Informationsaustausch unter den beteiligten Behörden ermöglichen und den Ermittlern auch analytische und forensische Hilfe leisten.

Die jüngsten Einsätze im Zuge der Operation Endgame liefen vom 19. bis 22. Mai 2025. In diesem Zeitraum haben die Behörden weltweit etwa 300 Server abgeschaltet, 650 Domains unschädlich gemacht und internationale Haftbefehle gegen 20 Zielpersonen erlassen, womit sie der Ransomware-Kill-Chain einen schweren Schlag versetzten.

1. Mit dieser Art Service kann man Telefonanrufe mit gefälschten oder sich ständig ändernden Telefonnummern tätigen oder E-Mails senden, die von einem gut beleumundeten Absender zu stammen scheinen

www.europol.europa.eu