European
Repository of
Cyber Incidents

# EuRepoC

# Cyber Conflict Briefing

**August 2023**

*Jakob Bund*
*Kerstin Zettl-Schabath*
*Martin Müller*
*Camille Borrett (Data Support)*

## Beobachtungen zur Gesamtlage

Im **August 2023** wurden 63 Cyber-Operationen in die EuRepoC-Datenbank aufgenommen. Das sind 26% mehr als im Vormonat, und 7 Operationen mehr als die insgesamt durchschnittlich verzeichnete Aktivität von 56 Cyber-Operationen pro Monat im Gesamtzeitraum.

Die durchschnittliche Intensität der im **August 2023** erfassten Operationen beträgt 2,81 und liegt somit über dem historischen Durchschnitt (2,6). Der auffällige Anstieg der Operationen seit Februar 2023 lässt sich vor allem auch dadurch erklären, dass EuRepoC ab diesem Zeitpunkt Cyberangriffe gegen Kritische Infrastrukturen grundsätzlich miteinschließt und nicht wie zuvor davon abhängig macht, ob diese Aktivitäten mit politischen beziehungsweise staatlichen Angreifern oder Opfern verknüpft sind.

## Über das Briefing

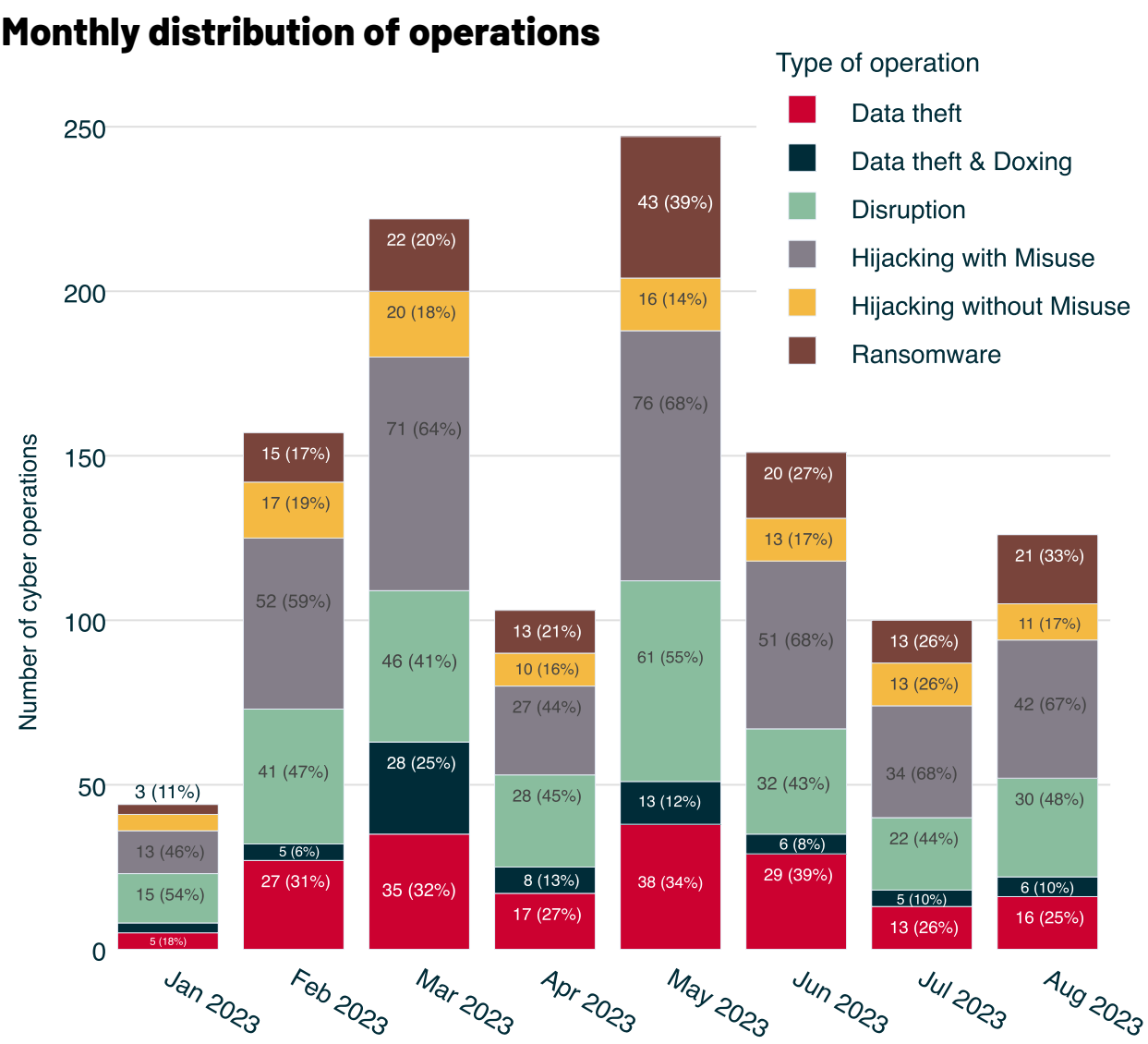
Analysen für das Cyber Conflict Briefing werden von EuRepoC erstellt. Die deutsche Ausgabe wird in Zusammenarbeit mit dem **Tagesspiegel Cybersecurity Background** veröffentlicht.
Das Briefing fasst die zentralen Trends, Dynamiken und Befunde zu den von EuRepoC in einem bestimmten Monat erfassten Cybervorfällen zusammen. Diese müssen nicht notwendigerweise im August stattgefunden haben, sondern können bereits zu einem früheren Zeitpunkt begonnen haben. Dabei stehen technische, politische sowie rechtliche Aspekte im Vordergrund.

## Über EuRepoC

Das European Repository of Cyber Incidents ist ein europäisches Forschungsprojekt mit dem Ziel, Informationen und Wissen über Cyber-Konflikte sichtbar zu machen. Es wird geleitet von der Universität Heidelberg, in Kooperation mit der Universität Innsbruck, der Stiftung Wissenschaft und Politik und dem Cyber Policy Institute (Estland). Es wird aktuell durch das Auswärtige Amt und das dänische Außenministerium gefördert.

Nähere Informationen zum EuRepoC-Projekt finden Sie hier.

Die im August 2023 erfassten Vorfälle verteilen sich auf folgende **Operationstypen**:




*Hinweis: Einzelne Cybervorfälle können mehrere Operationstypen in Kombination aufweisen.*

Der größte Anteil umfasst „Hijacking with Misuse"-Operationen (67%). Als Sammelbegriff fasst dies Aktionen, bei denen es Angreifern gelungen ist, in Systeme und Netzwerke einzudringen, um dort bereits unbefugt üblicherweise schädliche Aktionen auszuführen. Diese Aktivitäten werden, sofern erkennbar, weiter nach ihrer Absicht differenziert und können Datendiebstahl oder Betriebsstörungen umfassen.

So räumte die Greater London Metropolitan Police beispielsweise Ende August ein, dass persönliche Informationen von Polizisten und Polizistinnen sowie weiteren Angestellten bei einem externen Dienstleister, der für die Anfertigung von Dienstausweisen verantwortlich ist, entwendet wurden. Die nach der Lage ihres Hauptquartiers auch Scotland Yard genannte Polizeibehörde informierte alle 47.000 Beschäftigten über den möglichen Diebstahl von Fotos, Namen und anderen internen Erkennungsangaben. Verdeckte Ermittler und Ermittlerinnen wurden daraufhin als Vorsichtsmaßnahme von ihren Einsätzen abgezogen. Am 14. September gab die Polizeibehörde in Manchester bekannt, dass Daten ihrer mehr als 12.000 Mitarbeitenden, darunter 8.000 Polizeibeamten und -beamtinnen, ebenfalls von der Ransomwareattacke betroffen waren.

Der Vorfall betont erneut die Wichtigkeit, die Weitergabe von Daten auf zwingend notwendige Angaben zu minimieren – gerade im Kontakt mit externen Serviceanbietern – um Missbrauchsrisiken bei einer Datenpanne zu vermeiden. Im vorliegenden Fall waren zwar keine Privatadressen durch das Datenleck betroffen. Die Gefahr, dass die Identität von Sicherheitskräften offengelegt wird, zeigt gleichsam eine mögliche Schnittstelle zwischen finanziell motiviertem Doxxing durch kriminelle Gruppen und Desinformationsversuchen an.

Vorstellbar ist etwa, dass Ransomware-Akteure unter staatlichem Einfluss dazu instrumentalisiert werden, oder aus eigenem opportunistischem Handeln, Informationen in Umlauf bringen, die dazu geeignet sind als Teil von Desinformationskampagnen, Anfeindungen gegen und physische Konfrontationen von einzelnen Sicherheitskräften in deren privaten Umfeld zu provozieren. Angeblich oder tatsächlich ideologisch/terroristisch motivierte Gruppen könnten von diesen Informationen Gebrauch machen, um sogenannte “Kill-Lists” zu erstellen und zu Gewalt gegen gedoxxte Personen aufzurufen.

Der zweithäufigste im August verzeichnete Operationstyp waren „Disruption“-Operationen. Darunter verstehen sich Operationen mit dem Ziel, einen informationstechnischen Dienst außer Betrieb zu setzen. Eine Disruption oder Störung beeinträchtigt entsprechend dessen Verfügbarkeit. Störaktionen sind in aller Regel von vorübergehender Wirkung. Wir haben 30 davon erfasst.

Bereits Anfang Juli meldete die Hafenverwaltung von Japans größtem Frachthafen in Nagoya eine Ransomware-Attacke. Dadurch bedingte Betriebsausfälle beeinträchtigten über mehrere Tage hinweg die Containerlogistik. Eingeschränkte Möglichkeiten, Transporter zu be- und entladen sorgten für Verzögerungen in der Güterabfertigung am Hafen, der auch dem Autohersteller Toyota als Drehschreibe für die Verteilung von Bauteilen in seiner just-in-time Produktion dient. Zunächst der Ransomware-Gruppierung LockBit zugerechnet, äußerten hochrangige japanische Regierungsvertreter im August den Verdacht, staatlich gelenkte chinesische Akteure könnten für den Angriff verantwortlich sein. LockBit selbst betreibt ein Ransomware-as-a-Service-Modell und gewährt Zugriff auf seine Angriffswerkzeuge gegen Bezahlung beziehungsweise Beteiligung an erlangten Erpressungsgeldern. Nachdem im September 2022 ein ehemaliger Programmierer der Gruppe die grundlegenden Bausteine geleakt hatte, war es auch Akteuren ohne Verbindung zu LockBit möglich geworden, Ransomware-Operationen nach ähnlichem Verfahren durchzuführen.

Sollten sich die Verdachtsmomente hinsichtlich einer Beteiligung durch chinesische Gruppen erhärten, träte China damit in die Fußstapfen anderer staatlicher Akteure, in dem Versuch, eigene Verantwortung durch den Einsatz krimineller Instrumente zu verschleiern. Nordkorea und Russland hatten 2017 mit WannaCry und NotPetya durch die unkontrollierte Verbreitung von Ransomware für bis dahin beispiellosen wirtschaftlichen Schaden gesorgt.

In der Vergangenheit haben staatliche Akteure ebenfalls Ransomware verwendet, um durch das Auslöschen oder Verschlüsseln von Netzwerk- und Logdaten, andere zuvor ausgeführte Aktionen und das eigentliche Ziel einer Operation zu vertuschen. Ein fingierter Bezug zu LockBit, sofern im Fall von Nagoya zutreffend, wäre nicht nur ein Versuch Sabotage mit finanziellen Motiven zu tarnen, sondern eine False-Flag-Operation, die gezielt Aufmerksamkeit auf eine spezifische andere Gruppe lenkt. Angesichts internationaler Anstrengungen, wie der International Counter Ransomware Initiative, disruptiv gegen Ransomware-Gruppen und andere kriminelle Netzwerke vorzugehen, sind solche Nachahmungsversuche mit neuen Eskalationsrisiken verbunden.

## Brennpunkte und Zielmuster

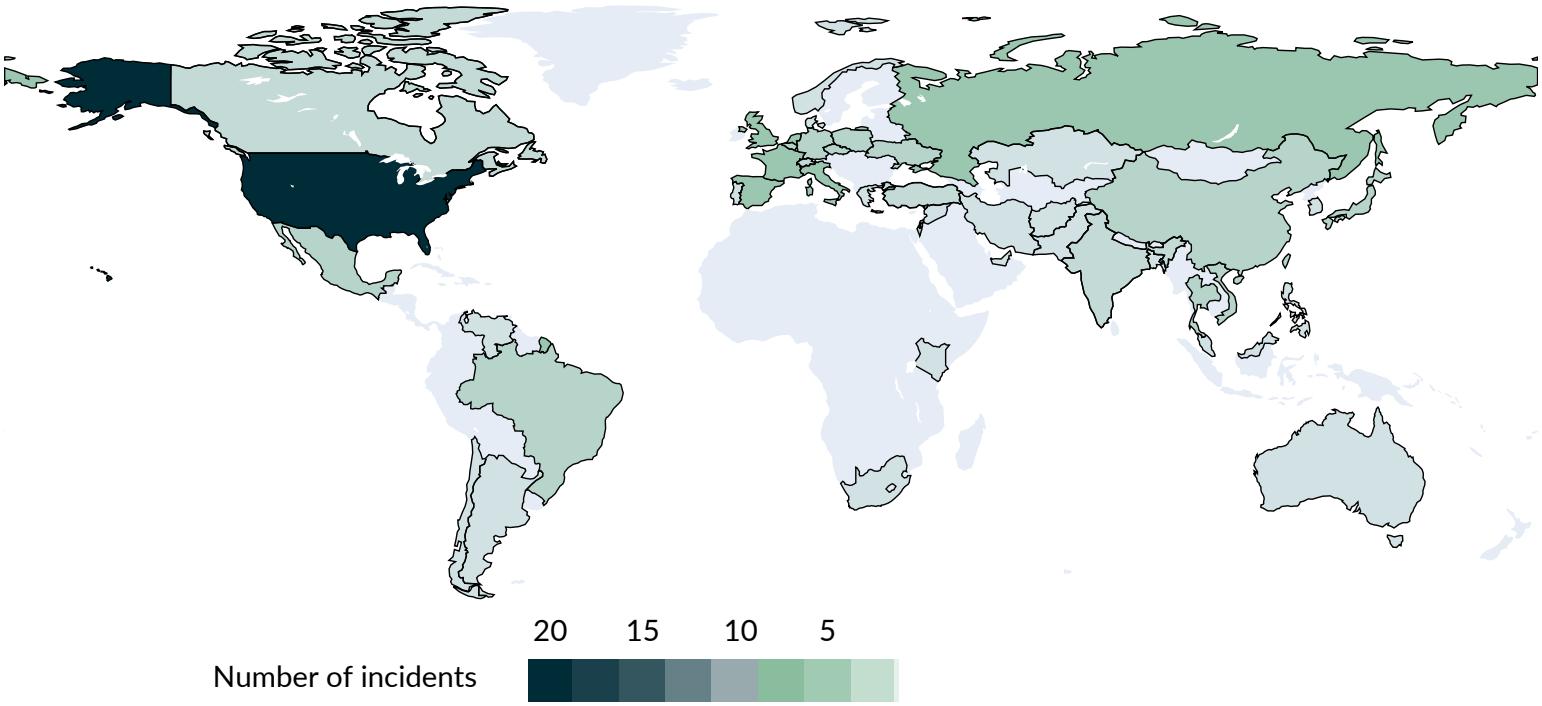
Der am häufigsten im August 2023 betroffene Zielsektor war, wie auch schon im Vormonat, Unternehmen der Kritischen Infrastruktur mit 36 Fällen beziehungsweise 57% der neu aufgenommenen Fälle. Dies stellt einen kleinen Anstieg im Vergleich zu den 31 Fällen im Juli dar, entspricht aber relativ der Menge gegenüber den Monaten Juni und Juli. Am zweithäufigsten betroffen waren in 26 Fällen (41%) staatliche Institutionen. Auch hier hat ein Anstieg (fast 37%) zum Vormonat stattgefunden, auf relativer Basis liegt die Zahl im Bereich der 40%-Marke der Vormonate.

Ein ähnliches Bild zeigt sich bei der Betrachtung der betroffenen Staaten: Erneut betraf etwa ein gutes Drittel der Vorfälle (insgesamt 22) die Vereinigten Staaten, was wir wie in den vergangenen Briefings auf die technologische und industrielle Dominanz im Cyberraum zurückführen.

Ähnlich oft mit 20 Fällen waren die Mitgliedsstaaten der EU betroffen, was gegenüber den vergangenen Monaten einen Anstieg darstellt, in denen der Anteil bei 20-25% lag. In diesem Monat war Italien mit sechs Fällen unter den EU-Staaten am häufigsten betroffen, gefolgt von Frankreich (vier Fälle) sowie Spanien und den Niederlanden mit jeweils drei Vorfällen. Deutschland war in zwei Vorfällen betroffen und damit wie schon im letzten Monat unterdurchschnittlich repräsentiert.

Für die im Datensatz aufgenommenen Vorfälle bei Unternehmen der kritischen Infrastruktur zeigt sich, dass der Gesundheitsbereich mit 10 Vorfällen erneut am häufigsten betroffen war. Dies betraf etwa in den USA mehrere Krankenhausbetreiber (etwa hier und hier), aber auch in Portugal und Belgien. Für den im letzten Monat am häufigsten betroffenen Finanzsektor wurden für August sechs neue Vorfälle registriert; für die Hälfte der Fälle ist dies auf “Diebstähle” bei Betreibern von Kryptowährungsbörsen (hier, hier und hier) zurückzuführen. Ebenfalls sechs Vorfälle betrafen den Transportsektor, zwei Drittel durch kurzlebige DDoS-Attacken pro-russischer Gruppen auf Ziele in EU-Mitgliedstaaten (näher dazu sogleich). Als deutlich schwerwiegender sind demgegenüber die den Gruppen ‘Akira’ bzw. ‘Play’ zugeschriebenen Ransomwarevorfälle bei der Belt Railway Company of Chicago respektive mehreren nicht näher genannten Managed Service Providern anzusehen.

## Geographic distribution of operations




Bei den staatlichen Institutionen zeigt sich erneut eine größere Vulnerabilität von lokalen beziehungsweise regionalen Behörden. Darunter sticht eine Anzahl von insgesamt zehn Bildungseinrichtungen heraus: Zwar wurden etwa für den Mai 14 den Bildungsbereich betreffende Vorfälle erfasst, allerdings bei einer gegenüber dem August fast doppelt so hohen Gesamtzahl der Fälle. Die Varianz der Vorfälle von Ransomwarevorfällen bei US- sowie Schweizer Institutionen über einen Fall von "CEO-Betrug" mit einem Schaden im Millionenbereich bis hin zum unerlaubten Zugriff auf E-Mail-Konten an der Heinrich-Heine-Universität in Düsseldorf verstärkt den Eindruck, dass Angreifende nach dem "Spray and Pray"-Prinzip gegen eine Vielzahl von Opfern vorgehen und bei IT-sicherheitsseitig schlechter ausgestatteten lokalen Behörden mehr Erfolg haben (siehe auch unser Briefing aus dem Vormonat).

Auf globaler Ebene sorgten drei Vorfälle für besondere Aufmerksamkeit: So wurde bekannt, dass sowohl die japanische Cybersicherheitsbehörde als auch Netzwerke des Verteidigungsministeriums mutmaßlich durch staatliche oder staatlich unterstützte chinesische Akteure ausgespäht wurden (zu letzterem Vorfall sogleich mehr). Zudem wurde bekannt, dass es unbekannten Angreifern gelungen war, in die Systeme der britischen Wahlbehörde einzudringen, was erst nach etwas über einem Jahr im vergangenen Oktober bemerkt wurde. Wenngleich wohl meist öffentlich bekannte Daten gestohlen wurden, wird vor einer weiteren Verwendung der Daten, etwa für gezielte Desinformationskampagnen im Zusammenhang mit Wahlen, gewarnt.

Die beiden Vorfälle mit deutschen Betroffenen umfassten neben dem unbefugten Zugriff auf die Email-Konten der Universität Düsseldorf noch einen durch eine Warnung des Verfassungsschutzes bekannt gewordenen Hack gegen den Exiliraner Mansour Sohrabi, für den die durch den Iran unterstützte Gruppierung "Charming Kitten" verantwortlich gemacht wird.


**Suspected countries of origin of initiators August 2023**

Number of operations per suspected initiating country

## Angreiferprofile und Attributionen

Auch im August pendelte sich der Prozentsatz der (noch) nicht konkreten Angreiferländern zugeordneten Cybervorfälle (Anzahl: 43) mit 68% um die 70% Marke ein. In 27 der 63 Fälle wurden nichtstaatliche Akteure verantwortlich gemacht, was prozentual einen leichten Anstieg von ca. 5% im Vergleich zum Vormonat Juli bedeutet. Von den 27 Vorfällen wurden 16 kriminell motivierten Akteuren zugesprochen, die übrigen 11 dagegen stärker ideologisch/politisch motivierten Hacktivisten. Sieben der 11 Hacktivisten-Operationen weisen eine russische Urheberschaft im Kontext des Kriegs gegen die Ukraine auf, was dessen auch noch 18 Monate nach Beginn starke Präsenz auch auf der Cyberebene unterstreicht. Für alle sieben Fälle zeichnete sich NoName057(16) verantwortlich, der neben KillNet aktivsten pro-russischen Hackergruppierung seit Anfang der Kampfhandlungen im Februar 2022. Acht der 13 im August konkreten konventionellen Konflikten zugeordneten Cybervorfälle drehten sich um den Krieg gegen die Ukraine.

Dabei stehen nach wie vor besonders die Ukraine unterstützende EU-Mitgliedstaaten im Kreuzfeuer der Hacktivistenoperationen, die sich im August gegen tschechische, spanische, niederländische und italienische Ziele richteten (7 der 7 NoName057(16)-Operationen). Die Zahl der sogenannten “Cyber-Proxies” zugesprochenen Vorfälle betrug im August in unserer Datenbank 9, mit davon fünf chinesischen Angreifern angelasteten Aktionen. Entsprechend rangiert China in der Liste attribuierter Angreifer-Herkunftsländer im August nur knapp hinter Russland, Nordkorea folgt wie im Vormonat Juli auf dem nächsten Platz.

Auffällig sind die zwei den USA zugeordneten Vorfälle, da US-amerikanische Cyberoperationen gemessen an ihrer vermuteten Anzahl nur selten publik werden. Die beiden Fälle spiegeln jedoch zwei bedeutende Aspekte wider, nämlich zum einen die nach wie vor hohe Gefahr von sogenannten “Insider-Aktionen” sowie die steigende Proaktivität demokratischer Strafverfolgungsbehörden, wenn es um die operative Stilllegung/Zerschlagung von Hacking-Netzwerken/Infrastrukturen geht.

So wurde bekannt, dass ein Ingenieur der Arnold Air Force Base in Tennessee (USA) zum einen Hardware mit nach Hause genommen und sich zum anderen mutmaßlich Zugang zu Kommunikation des FBI und verschiedener staatlicher Behörden Tennessees verschafft hatte. Bereits Mitte Juni wurde ein Mitglied der Massachusetts Air National Guard angeklagt, da er sensible Pentagon-Informationen über seinen privaten Discord-Server veröffentlicht hatte, inklusive brisanten Informationen zur Einschätzung des Ausgangs des Kriegs gegen die Ukraine seitens des US-Militärs. Diese Beispiele zeigen einmal mehr, dass gerade in hochsensiblen Bereichen entsprechend des immer häufiger propagierten "Zero-Trust"-Ansatzes nicht nur davon ausgegangen werden sollte, dass bereits externe Akteure Zugang zu den eigenen Netzwerken erlangt haben, sondern dass auch eigene Mitarbeiter zu einem potenziellen Sicherheitsproblem werden könnten. Der zweite Fall mit US-Urheberschaft demonstriert dagegen den verstärkt angewandten Ansatz einer "aktiven Cyberabwehr" seitens staatlicher Strafverfolgungsbehörden, wie er aktuell auch für die EU diskutiert wird: wie bereits zuvor in anderen Fällen hatten zahlreiche Strafverfolgungsbehörden, unter Leitung des FBI und Beteiligung des BKA, das sog-"Qakbot"-Botnetz/Schadsoftware, bzw. dessen Infrastruktur unschädlich gemacht. Nach Angaben des FBI existierte Qakbot bereits seit 2008 und wurde seither für Ransomware und weitere Cybercrime-Aktivitäten weltweit genutzt. In der koordinierten Strafverfolgungsoperation erlangte das FBI Zugriff zur Qakbot-Infrastruktur, leitete deren Traffic um und konnte so letztlich durch die Installierung einer "uninstaller"-Datei auf den infizierten Computern diese vom restlichen Botnetz trennen und die Installierung weiterer Malware verhindern.

Wie bereits beschrieben, ist dies aus technischer Sicht jedoch nicht mit der Bereinigung der bereits infizierten Computer von potenzieller anderweitiger Malware anzusehen, lediglich deren Zugehörigkeit zum Qakbot-Botnetz wurde somit zerschlagen. Der Fall demonstriert den steigenden Willen zu internationaler Koordination zwischen Strafverfolgungsbehörden, um Cyber-Crime-Gruppierungen großflächiger und effektiver begegnen zu können und deren Kosten zur Durchführung ihrer Operationen auf lange Sicht so stark in die Höhe zu treiben, dass sich ihr Geschäftsmodell nicht mehr lohnt. Strafverfolgungsaktionen, die einen Zugriff auf die Systeme der Opfer der Cyber-Crime-Gruppierungen erfordern, stellen aus rechtlicher Sicht jedoch eine noch größere Herausforderung dar als Operationen, die lediglich Zugriff zu den Angreifer-Infrastrukturen benötigen, etwa im Falle der konzertierten Aktion gegen die Ransomwaregruppe Hive, die Anfang dieses Jahres bekannt geworden war. Für sämtliche solcher Operationen stellt sich jedoch die Frage der langfristigen Effektivität ohne zeitgleich erfolgende Inhaftierung der verantwortlichen Personen hinter der Technik, da z.B. auch die Schadsoftware Emotet nach einer erfolgreichen Strafverfolgungsoperation Anfang 2021 gegen sie letztlich nur kurze Zeit später wieder detektiert wurde.

In vier der 38 Fälle, in denen ein konkreter Attributionsakteur identifiziert werden konnte, handelte es sich um US-Behörden. So attribuierte das FBI zwei, die NSA einen und das US Department of Justice ebenfalls einen weiteren Fall im August aus unserem Datensatz.

Auch wenn diese Zahlen z.B. gegenüber der Anzahl durch Threat Intelligence Unternehmen attribuierten Vorfälle (12 im August) deutlich geringer erscheint, lohnt sich ein genauerer Blick auf die Fälle: Die zwei FBI-Attributionen (Selbstattribution der Qakbot-Aktion sowie Attribution einer Lazarus-Kampagne) wurden beide in Form von politischen Statements auf den Behörden-Webseiten veröffentlicht. Eine politische Attribution, die durch offizielle Kanäle erfolgt, ist mit stärkerem "Gewicht"/Formalität versehen. Gleichzeitig stellt sie an die attribuierende Regierung jedoch auch andere Erwartungen hinsichtlich möglicher Folgehandlungen, als "informelle" Attributionen, wie die durch einen Washington Post Artikel vom 7. August "durchgestochene" Attribution chinesischer Hackingoperationen gegen japanische Ziele durch die NSA. Dieses "Durchstechen" kann unterschiedliche Motivlagen haben. Im vorliegenden Fall könnte es der bewusste Versuch sein, noch stärkeren öffentlichen Druck auf einen verbündeten Staat auszuüben, die eigenen und damit potenziell auch die US-Systeme effektiver im Cyberspace zu schützen, ohne dabei einen offiziellen Weg beschreiten zu müssen. Ohne geteilte Vorstellungen oder sogar Regeln darüber, wann, wie und warum demokratische Regierungen in welchen Fällen offizielle Attributionen von Cyberoperationen vornehmen, kann über die genauen Motivlagen und Beweggründe zumeist nur spekuliert werden, was jedoch eine Bewertung des "Erfolgs" einer Attribution ohne Kenntnis des angestrebten Ziels durch Außenstehende erschwert.

## Mehr von EuRepoC

In einem umfangreichen Redesign hat das European Repository die Möglichkeiten, Cyberoperationen interaktiv zu erforschen, erweitert. Eine neu gestaltete Website bietet seit dem 27. September Zugang zu benutzerdefinierten Funktionen, die eine dynamische Visualisierungen von Trends in der Cyberbedrohungslandschaft erlauben.

In einer Besprechung der neuen Nationalen Sicherheitsstrategie weisen Annegret Bendiek und Jakob Bund auf die Notwendigkeit hin, parlamentarische Kontrollmöglichkeiten von Beginn in Überlegungen über neue Befugnisse für die Cyberabwehr einzubeziehen. Voraussetzung dafür, vorgeschlagene Maßnahmen in ihrer Eignung zu überprüfen, ist – wie der Kommentar hervorhebt – zudem eine vorausgehende Bestimmung der strukturellen Besonderheiten von Cyberbedrohungen.

In einem weiteren APT-Profil befassen sich das EuRepoC-Team mit der chinesischen Gruppierung APT3/Boyusec, die als private Firma getarnt im Auftrag des Ministerium für Staatssicherheit Industriegeheimnisse ausspähte. APT3 stach unter anderem durch die Zusammenarbeit mit staatlichen Prüfstellen hervor, über welche die Gruppierung mutmaßlich Zugang zu Informationen über neu entdeckte Schwachstellen erhielt.

Darüber hinaus informiert EuRepoC mit einem täglich kuratierten Cyber Incident Tracker über neu in die Datenbank aufgenommene Cybervorfälle. Diesen können Sie hier abonnieren.


### Über die Autor:innen

**Jakob Bund** ist Wissenschaftler an der Stiftung Wissenschaft und Politik (SWP).

**Kerstin Zettl-Schabath** ist Wissenschafterin am Institut für Politische Wissenschaft (IPW) der Universität Heidelberg.

**Martin Müller** ist Universitätsassistent und Dissertant am Institut für Theorie und Zukunft des Rechts an der Universität Innsbruck.

**Camille Borrett** ist Datenanalystin an der Stiftung Wissenschaft und Politik (SWP).