European
Repository of
Cyber Incidents

# EuRepoC

# Cyber Conflict Briefing

**Mai 2023**

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

## Beobachtungen zur Gesamtlage

Im **Mai 2023** wurden 112 Cyber-Operationen in die EuRepoC-Datenbank aufgenommen. Das sind 77.8% mehr als im Vormonat, und 52 Operationen mehr als die insgesamt durchschnittlich verzeichnete Aktivität von 60 Cyber-Operationen pro Monat im Gesamtzeitraum.

Die durchschnittliche Intensität der im Mai 2023 erfassten Operationen beträgt 3,13 und liegt somit über dem historischen Durchschnitt (2,5). 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. Die im Vergleich zum März und April im Mai deutlich erhöhte Anzahl an verzeichneten Cyberoperationen erscheint dennoch eine bemerkenswerte Auffälligkeit zu sein.

## Über das Briefing

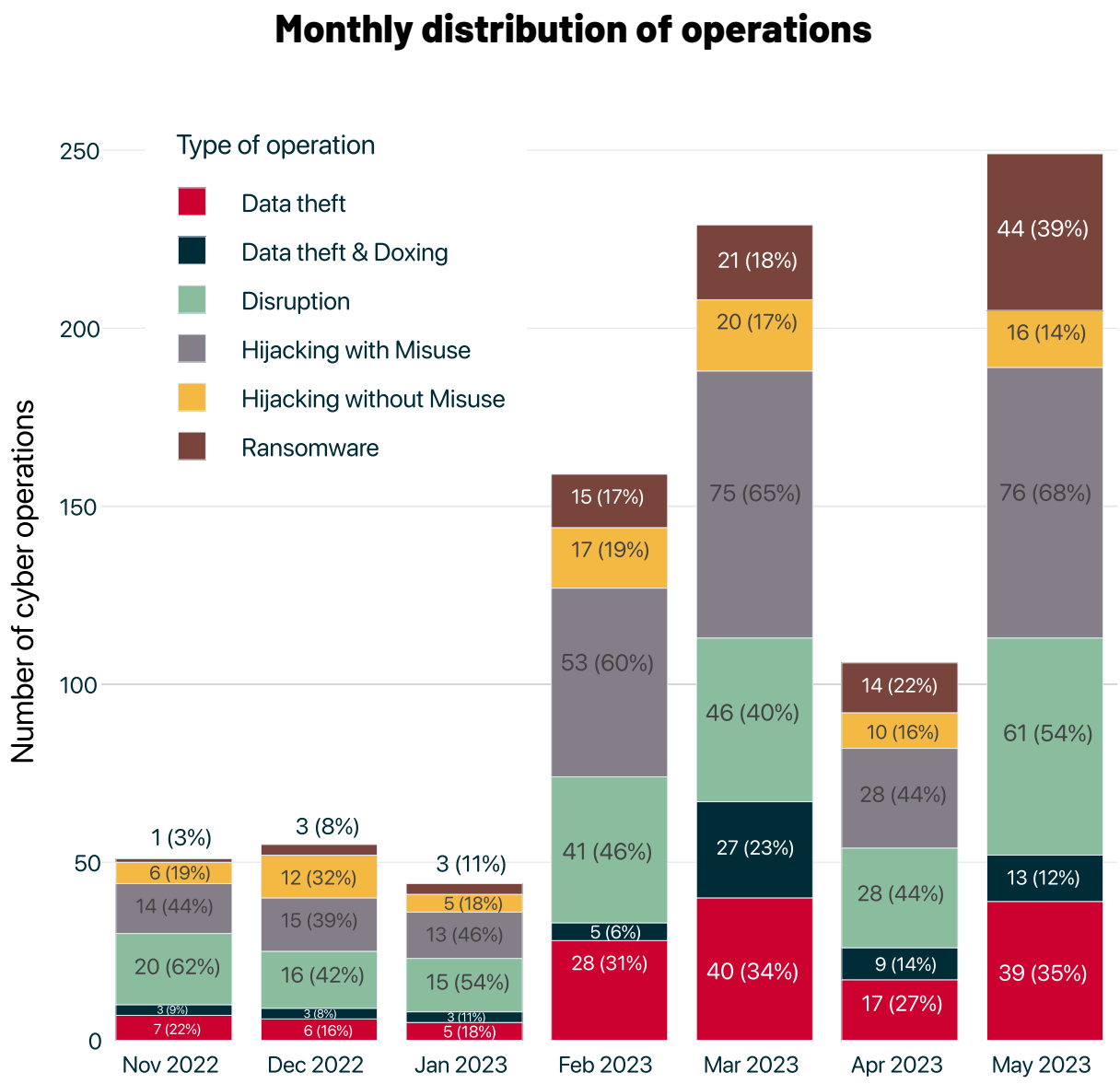
Analysen für das Cyber Conflict Briefing werden von EuRepoC erstellt. Die deutsche Ausgabe wird in Zusammenarbeit mit dem **Tagesspiegel Cybersecurity Background** veröffentlicht.
Das Briefing fasst die zentralen Trends, Dynamiken und Befunde zu den von EuRepoC in einem bestimmten Monat erfassten Cybervorfällen zusammen. Diese müssen nicht notwendigerweise im Mai 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 Mai 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 (76%). 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.

Hervorhebenswert in diesem Zusammenhang sind im Mai die durch Microsoft und den Geheimdienstverbund der Five-Eyes-Staaten am selben Tag (24.5.) offengelegten Aktionen von Volt Typhoon (auch bekannt als BRONZE SILHOUETTE/Vanguard Panda), einer Gruppe mit mutmaßlichen Verbindungen zur chinesischen Regierung.

Konkret haben sich diese Ausspähaktionen gegen Kritische Infrastrukturbereiche in den USA gerichtet. Die für den Bericht verantwortlichen Behörden gehen davon aus, dass ähnliche Techniken auch weltweit zum Einsatz kommen könnten. In einer eigenständigen Bewertung gelangt Microsoft zu der Einschätzung, dass die beobachteten Unternehmungen darauf abzielen, Erkenntnisse zu sammeln, um wichtige Kommunikationswege zwischen den USA und Asien im Falle einer zukünftigen Krise abschneiden zu können.

Volt Typhoon zeichnet sich durch die Verwendung von sogenannten „Living-off-the-Land"-Taktiken aus. In Anlehnung an die Ausbeutung von eroberten Landstrichen durch napoleonische Truppen strebt dieser Ansatz an, den eigenen Vormarsch von Versorgungslinien unabhängig zu machen. Anstelle der Plünderung von Kornspeichern spielt im Kontext von Cyberoperationen insbesondere die geschickte Verwendung von Werkzeugen, die von den Zielen selbst zur Netzwerkverwaltung im Einsatz sind, eine Rolle. Diese Taktiken dienen vorrangig dazu, Angriffsaktionen unscheinbar in den typischen Datenverkehr und normales Nutzungsverhalten einfließen zu lassen und so eine Entdeckung möglichst lange zu verhindern.

Auch nach Bekanntwerden und der Dokumentation von Anzeichen einer Kompromittierung kann diese Vorgehensweise die Entdeckung von Angreifern vor anhaltende Herausforderungen stellen. Gerade die Unterscheidung von legitimem und bösartigem Verhalten verlangt eine genaue Kenntnis der üblichen Netzwerkbewegungen, die in der Verantwortung potenzieller Ziele liegt, um eventuell falsch-positive Warnungen einordnen zu können.

In einer neuen Entwicklung hat die Ratingagentur Moody's zum ersten Mal eine behördliche Cybersicherheitswarnung zum Anlass genommen, die dargestellten Risiken als unmittelbar kreditschädigend für die US-Kommunikations-, Energie- und Transportsektoren zu bewerten. Grund dafür seien die im Rahmen einer Störung zu erwartenden Einnahmen- und Liquiditätsminderungen, aber auch längerfristige Reputationsschäden, Rechtsstreitigkeiten oder – und bemerkenswerterweise unabhängig vom tatsächlichen Eintreten eines Schadensfalls – Risiken verstärkter regulatorischer Aufsicht.

Der zweithäufigste im Mai 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. Zum einen weil Angreifer dadurch versuchen das Eskalationsrisiko einzudämmen, zum anderen weil die zahlenmäßige Mehrheit von Operationen auf DDoS-Angriffe entfällt, die Webseiten nur für die begrenzte Dauer ihrer lawinenartigen Zugriffsanfragen überwältigen. Ebenfalls häufig verzeichnet werden sogenannte "Defacement"-Angriffe, bei denen Webseiten nicht nur lahm gelegt, sondern auch mit zumeist politisch/ideologisch motivierten Inhalten "verunstaltet" werden. Technisch anspruchsvollere Operationen, wie Ransomware-Angriffe, die betriebswichtige Daten verschlüsseln oder gezielte Sabotage-Aktionen können aber auch für längerfristige Ausfälle oder in äußerst seltenen Fällen permanenten (auch physischen) Schaden sorgen.

Von diesen Aktionen mit Störabsicht hat EuRepoC für Mai insgesamt 61 erfasst, darunter war jedoch kein Vorfall mit physischen Effekten/Schäden, was auf die Dominanz weniger intensiver DDoS-/Defacement-Operationen im Vergleich zu Sabotage-Akten hindeutet.

Abweichend von der Maße an Maßnahmen mit dem Ziel Schaden zu verursachen, werden Störaktionen auch zu Cybersicherheitszwecken durchgeführt. Die Zerschlagung von Angriffsinfrastruktur der russischen Spionagegruppe Turla durch das FBI Anfang Mai ist ein Beispiel für solches operationelles Eingreifen, um Angriffe zu verhindern.

Turla wird von der US-Regierung einer Einheit des russischen Inlandsgeheimdienstes FSB zugeschrieben und gilt als einer der ältesten kontinuierlich aktiven Cyberakteure. Über 20 Jahre unterhielt die Gruppe ein durch die Schadsoftware Snake weltweit verknüpftes Spionagenetzwerk. Snake ist tief in infizierten Systemen und Netzwerken versteckt. Zuletzt war die Schadsoftware auf mehreren hundert Computern in über 50 Ländern aktiv. Turla entwickelt das Werkzeug regelmäßig weiter und aktualisiert es auf durch die Gruppe kontrollierten Zielsystemen, um eine Offenlegung zu vermeiden.

Darüber ist es Turla in der Vergangenheit gelungen, Informationen über eine Reihe von Stationen in diesem Netzwerk lange unentdeckt auszuschleusen. In Deutschland gab das Auswärtige Amt 2018 einen Cyberangriff bekannt, den Medienberichten mit Snake in Verbindung brachten.

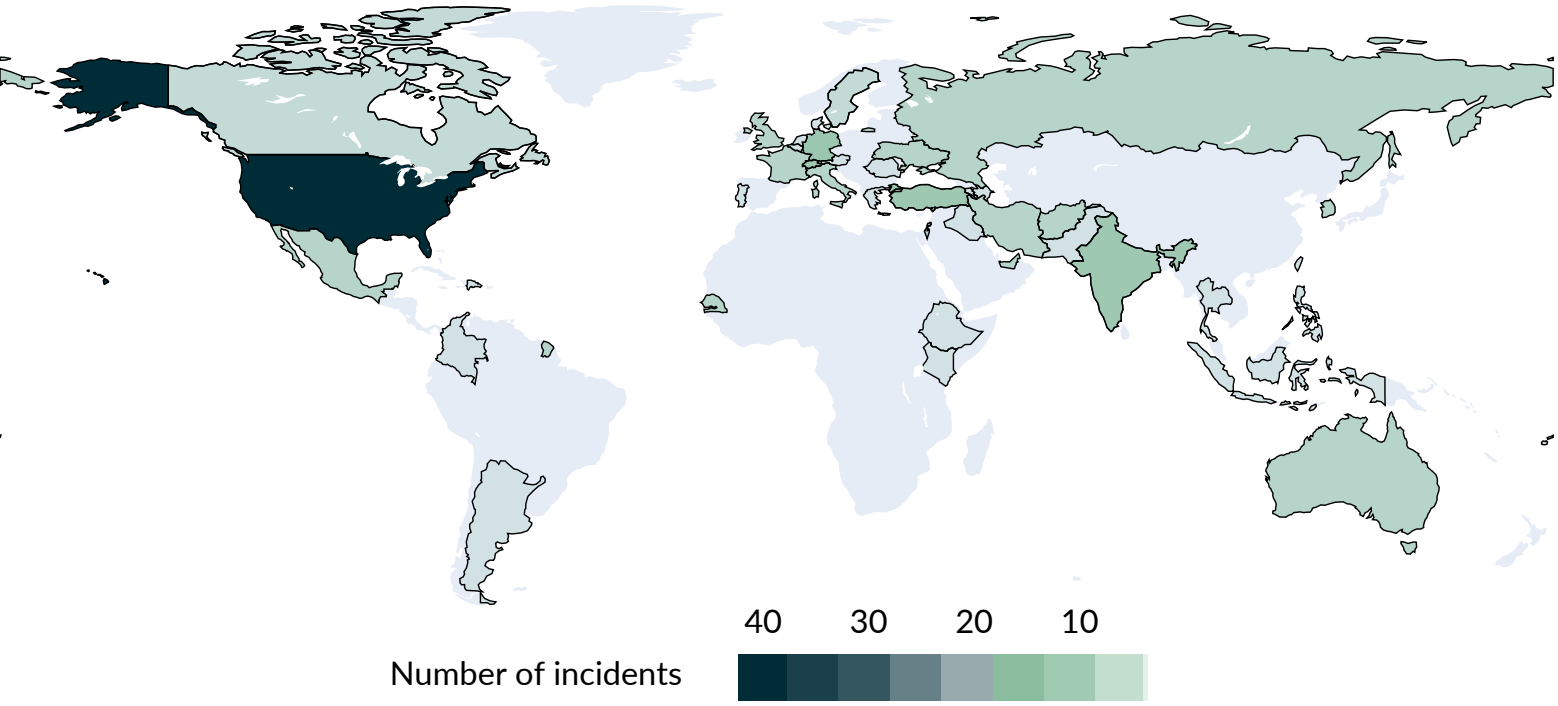
Nach gemeinsamer Beobachtung mit Verbündeten und privatwirtschaftlichen Partnern erwirkte das FBI am 8. Mai einen Durchsuchungsbeschluss, der es Ermittlern erlaubte, ein eigens entwickeltes Programm auf infizierte Systeme in den USA zu spielen. Die FBI-Software bringt Snake dazu, sich selbst zu überschreiben und damit zu neutralisieren.

Dieses Vorgehen weist auf Weiterentwicklungen im Gebrauch von Ermittlungs- und Strafverfolgungsmethoden hin, die sich nicht mehr allein darauf konzentriert, verantwortliche Täter zu belangen, sondern zunehmend auch darauf, Angriffsfähigkeiten von Bedrohungsakteuren zu schwächen, um deren Taten vorzubeugen oder zumindest in ihrer Schadenswirkung zu mindern.

## Brennpunkte und Zielmuster

Ein Blick auf die Verteilung der Cybervorfälle auf die jeweilig betroffenen Staaten zeigt - wie in den Monaten zuvor auch - dass die Vereinigten Staaten mit Abstand am häufigsten betroffen waren. Im Mai waren es fast ein Drittel der Operationen (40), was in etwa dem Anteil der Vormonate entspricht. Am zweithäufigsten war Deutschland durch sechs Vorfälle betroffen und damit auch der am häufigsten anvisierte EU-Mitgliedstaat, ebenfalls wie bereits im Vormonat. Insgesamt waren EU-Mitgliedsstaaten in ungefähr einem Fünftel aller Vorfälle (25) unter den berichteten Zielen. Die Verteilung spiegelt den im Vergleich deutlich vergrößerten Angriffsvektor der USA im Cyberspace wider, was sich vor allem durch deren Dominanz im industriellen sowie technologischen Bereich begründen lässt.

## Geographic distribution of operations

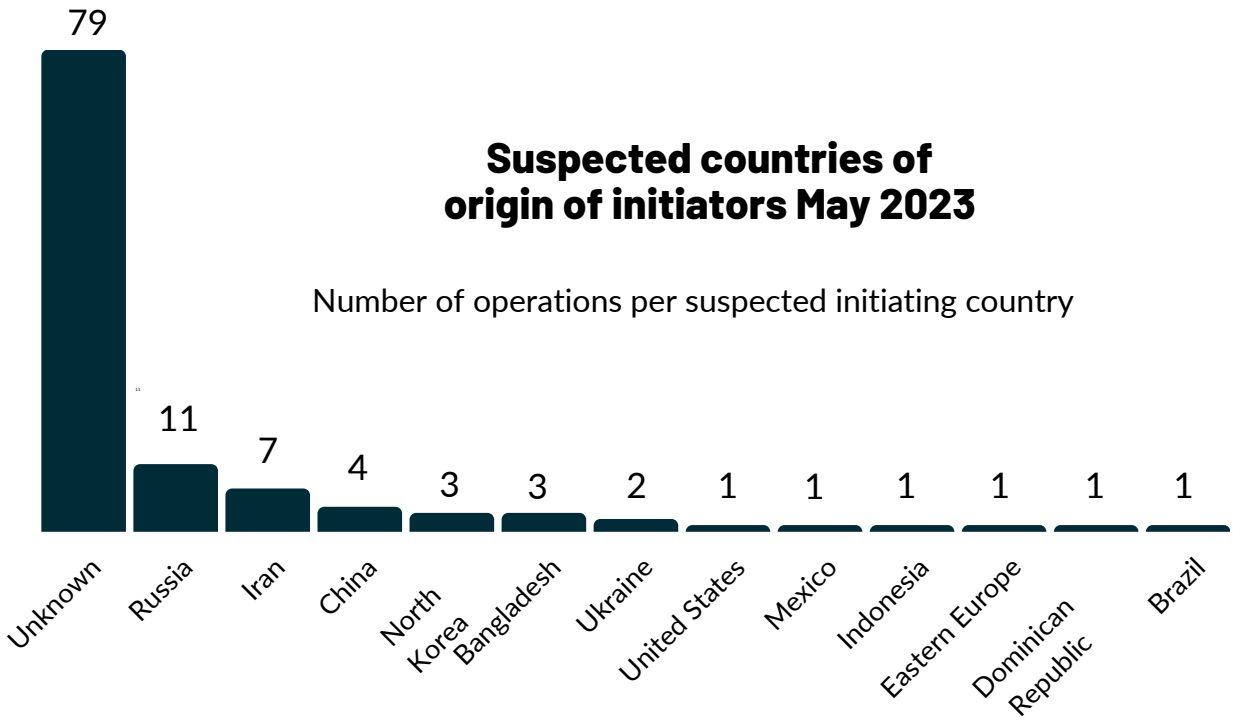



Je mehr erfolgreiche und für Cyberspionage, aber auch Ransomware-Operationen attraktive Unternehmen und Institutionen ein Land aufweist, desto häufiger werden diese potenziell auch zum Ziel von Cyberangriffen. Abschließend kommt noch die herausragende (geo-)politische Stellung der USA hinzu, was neben kommerziellen Motivlagen von Cybercrime-Gruppen auch politisch motivierte Angriffe begünstigt.

Im Mai 2023 waren erneut kritische Infrastrukturen mit 56 Fällen in knapp der Hälfte der aufgenommen Fälle betroffen, was sich aus absoluter Sicht jedoch mit der Anzahl der Fälle des Vormonats (50) deckt. Dicht dahinter rangieren mit 54 Fällen oder 48% der Gesamtfälle staatliche Institutionen als betroffene Sektoren, was eine merkliche Steigerung gegenüber den 22 Fällen des Vormonats darstellt. Unter den Fällen in denen (auch) EU-Mitgliedstaaten betroffen waren, fanden sich für die Kritischen Infrastrukturen mit fünf verzeichneten Fällen im Mai am häufigsten Angriffe gegen den Subsektor des “Critical Manufacturing”, ein Bereich, der besonders häufig von Supply-Chain-Operationen betroffen ist.

Dies betraf in Deutschland etwa das Rüstungsunternehmen Rheinmetall und den Kfz-Ersatzteilhändler Bilstein Group. Beiden Fällen gemein ist, dass die Fälle bekannten Ransomwaregruppierungen zugeschrieben werden und - soweit ersichtlich - nicht von staatlichen Akteuren durchgeführt wurden.

Bei den in ähnlicher Häufigkeit betroffenen staatlichen Zielen zeigt sich, dass in 14 Fällen Bildungseinrichtungen oder zugehörige Verwaltungsbehörden, wie etwa das Erziehungsdepartement in Basel-Stadt in der Schweiz betroffen waren. Einhergehend damit sind auch regionale und lokale Behörden überproportional betroffen. Hier liegt auch angesichts der häufig unbekannten Angreifenden die Vermutung nahe, dass in diesen Bereichen die Absicherung gegen Cyberangriffe auf einem niedrigeren Standard als bei Behörden auf nationaler Ebene liegt und deshalb an sich “nicht-zielgerichtete” Attacken von Cyberkriminellen - teils unter Einsatz von Ransomware, teils ohne - erfolgreicher sind.




## Angreiferprofile und Attributionen

Auch im Mai zeigt sich der Trend auf Angreiferseite, dass die Mehrzahl der verzeichneten Operationen bislang noch keinem Ursprungsland zugeordnet wurde (79 von 112 Fällen). Ferner etablieren sich Hackergruppierungen russischen Ursprungs auch in diesem Monat als die am häufigsten für Cyberangriffe verantwortlich gemachten Akteure, mit diesmal 11 Fällen und somit einem weniger als im Vormonat April.

Nachdem der Iran im April bereits im Vergleich zum März in der Angreiferliste sehr viel weiter oben positioniert war, nahm er im Mai mit 7 zugeordneten Fällen diesmal sogar direkt hinter Russland den zweiten Platz ein. Operationen, die ukrainischen Akteuren zugesprochen wurden, fallen im Mai im Vergleich zum Vormonat (5) mit nur zwei Vorfällen leicht ab.

Alle vier Operationen, die chinesischen Akteuren zugesprochen wurden, beziehen sich auf sogenannte “Advanced Persistent Threats” (APTs), zumeist von Staaten beauftragte/unterstützte Hackergruppierungen.

Wie in der Vergangenheit für chinesische Gruppierungen zumeist beobachtet handelte es sich dabei um Cyberspionage-Fälle mit bereits verzeichnetem Datendiebstahl oder aber der bislang lediglich nachgewiesenen Infiltration von Zielsystemen, was nicht nur für späteren Datendiebstahl, sondern im Falle von eskalierenden Konflikten auch als Einfallsvektor für Sabotage-Operationen genutzt werden könnte. Genau diese Befürchtung äußerte Microsoft in dem bereits erwähnten Bericht zu den Operationen der chinesischen APT Volt Typhoon. Einschätzungen darüber, welche Absicht(en) ein Angreifer tatsächlich mit einer Kompromittierung eines Netzwerkes auf längere Sicht verfolgt, gestalten sich zumeist äußerst schwierig und erfolgen oftmals unter Zuhilfenahme weiterer, geopolitischer Kontextfaktoren, wie etwa der Beziehung zwischen dem angegriffenen und dem Angreiferland, was auch hier der Fall gewesen zu sein scheint. Dass das Joint Cybersecurity Advisory der Five-Eyes-Staaten direkt auf den Microsoft-Bericht verweist, deutet neben dem Timing der Veröffentlichung auf eine intensive öffentlich-private Koordination im Vorfeld der Publikationen hin.

Im Gegensatz zu Microsoft halten sich die Behörden jedoch mit Aussagen zu den mutmaßlichen Absichten der chinesischen Hacker zurück und fokussieren sich auf die Offenlegung der “Indicators of Compromise” (IOCs) sowie die Beschreibung potenzieller Präventiv-/Gegenmaßnahmen. Man könnte dies als eine Art arbeitsteilige Attributionspraxis beschreiben, in der die staatlichen Behörden die politisch brisanteren Aussagen dem privaten Unternehmen überlassen und sich selbst stärker auf den Aspekt der Resilienzstärkung fokussieren.

Auffällig in der Liste der attribuierten Ursprungsländer ist ferner Bangladesch mit drei Vorfällen. Weder im März noch im April war das Land in der Liste vertreten. Verantwortlich für diese Veränderung ist das Auftreten der Hacktivisten-Gruppierung “Mysterious Team Bangladesh”. Erstmals öffentlich in Erscheinung trat sie 2022, durch DDoS-Angriffe auf vor allem indische Ziele. Zwischen Indien und Bangladesch existieren Grenzkonflikte, Streitigkeiten um wichtige Ressourcen wie Wasser, sowie auch religiöse Animositäten. Eine solche Gemengelage macht patriotische oder ideologisch motivierte Hacktivisten-Operationen wahrscheinlicher und kann das indische Zielprofil erklären. Weniger plausibel erscheint dagegen die Fokussierung der Gruppierung auf vor allem äthiopische und senegalesische Institutionen im Jahr 2023, genauer gesagt in zwei der drei Vorfällen vom Mai: So ist öffentlich kein konkreter Konflikt oder Disput zwischen den Ländern bekannt, was aufgrund der geografischen Distanz auch weniger wahrscheinlich ist.

Hacktivisten-Angriffe richten sich zumeist gegen regionale Rivalen des eigenen Heimatlandes und seltener gegen Länder aus anderen Regionen, zudem sollten diese nicht als proaktives Unterstützer-Land verfeindeter Staaten gelten. Wahrscheinlicher handelte es sich hierbei daher um opportunistische Aktionen gegen nicht ausreichend geschützte Ziele, um die eigenen Fähigkeiten zu demonstrieren und Aufmerksamkeit zu erzeugen.

Im Mai wurden mit 7 Vorfällen deutlich weniger Operationen dem Krieg Russlands gegen die Ukraine zugeordnet. Im April waren es noch 15 Vorfälle gewesen. Drei der Operationen betrafen Staaten, die die Ukraine unterstützen (Italien, Frankreich, Niederlande) und sich nach wie vor vor allem DDoS-Operationen pro-russischer Hacktivisten-Gruppierungen, wie in diesem Falle der Gruppierung NoName057(16), ausgesetzt sehen. Am zweithäufigsten (4) wurden die geopolitischen Spannungen zwischen dem Iran und Israel Cybervorfällen im Mai zugeordnet. Besonders iranische APTs zielen mit ihren Operationen immer wieder darauf ab, sensible Informationen öffentlicher und privater israelischer Institutionen zu erbeuten. In einem Fall tarnte die Gruppe Agrius dabei ihre Operation als angebliche Ransomware-Operation, eine immer häufiger verzeichnete Taktik staatlich-unterstützter Gruppierungen, die destruktive, politisch motivierte Angriffe hierdurch verschleiern wollen.

## Mehr von EuRepoC

In einem Anfang Juni veröffentlichten Arbeitspapier des EuRepoC-Konsortialmitglieds Stiftung Wissenschaft und Politik beschäftigte sich Mika Kerttunen aus militär-theoretischer und operativer Perspektive mit der Frage, inwiefern der Einsatz von militärischen Cyberfähigkeiten bereits einen Kriegszustand konstituiert. Als empirischer Fall wird darin besonders auch der aktuelle Einsatz von Cyberoperationen im Rahmen des Kriegs gegen die Ukraine diskutiert.

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).

## Follow us on social media