European
Repository of
Cyber Incidents

EuRepoC

Cyber Conflict Briefing

April 2023

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

Beobachtungen zur Gesamtlage

Im **April 2023** wurden 63 Cyber-Operationen in die EuRepoC-Datenbank aufgenommen. Das sind -28,41% weniger als im Vormonat, jedoch immer noch 15 Operationen (31,25%) mehr als die insgesamt durchschnittlich verzeichnete Aktivität von 48 Cyber-Operationen pro Monat.

Die **durchschnittliche Intensität** der im April 2023 erfassten Operationen beträgt 2,81 und liegt somit über dem historischen Durchschnitt (2,7). 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

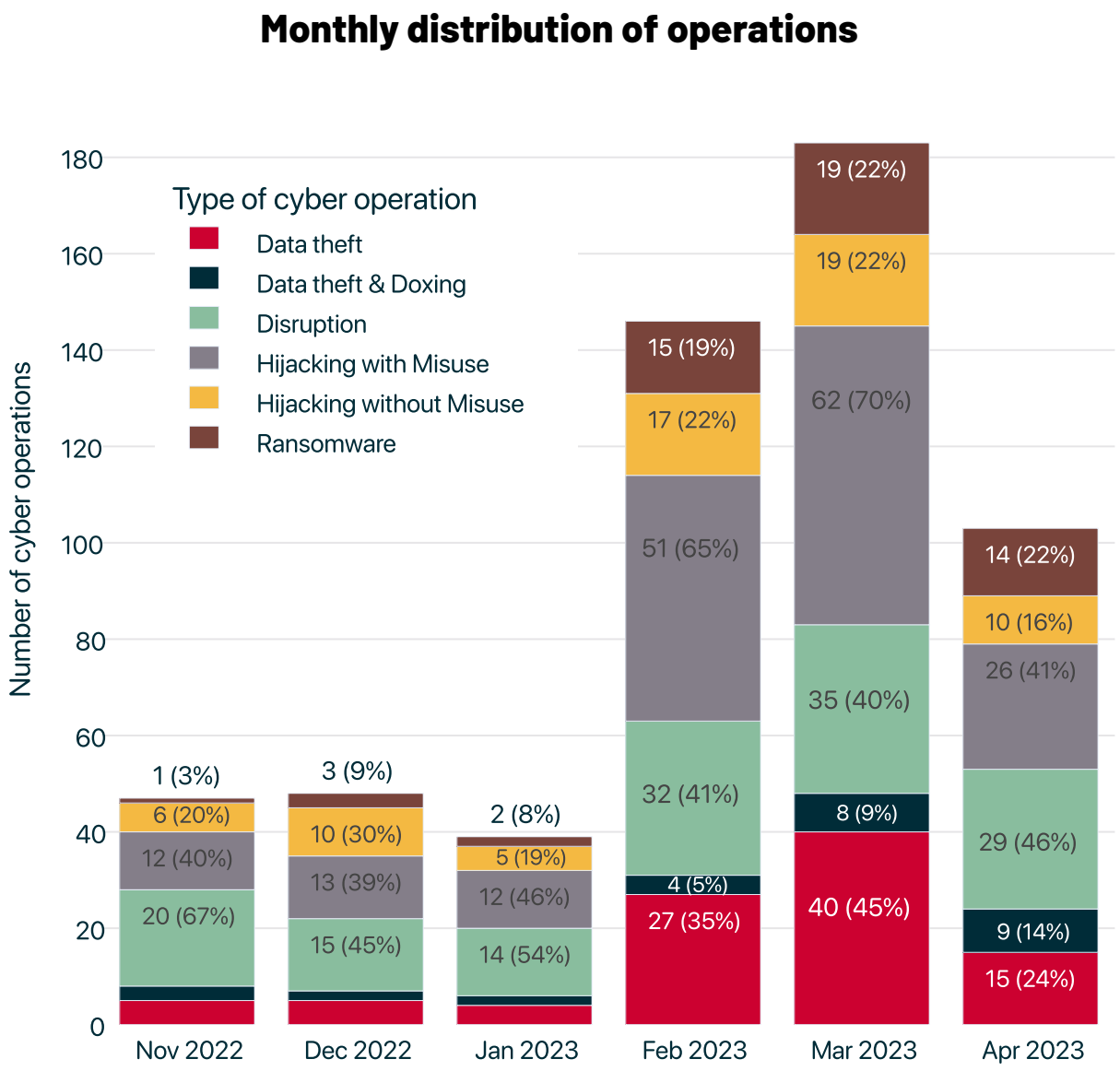
Analysen für das Cyber Conflict Briefing werden von EuRepoC erstellt. Die deutsche Ausgabe wird in Zusammenarbeit mit dem **Tagesspiegel Cybersecurity Background** veröffentlicht.
Das Briefing fasst die zentralen Trends, Dynamiken und Befunde zu den von EuRepoC in einem bestimmten Monat erfassten Cybervorfällen zusammen. Diese müssen nicht notwendigerweise im April 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 April 2023 erfassten Vorfälle verteilen sich auf folgende **Operationstypen**:



Hinweis: Einzelne Cybervorfälle können mehrere Operationstypen in Kombination aufweisen.

Der größte Anteil umfasst **„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, können aber auch für längerfristige Ausfälle oder in äußerst seltenen Fällen permanenten Schaden sorgen. Typische Beispiele für Störungen sind DDoS-Angriffe, die meist öffentlich anwählbare Webseiten ins Visier nehmen und durch eine Flut von Zugriffsanfragen, die Server, über die Internetseiten laufen, in die Knie zwingen und diese zeitweise unzugänglich machen.

Technisch anspruchsvoller sind **Ransomware-Attacken**, die Daten in erpresserischer Absicht verschlüsseln und das Arbeiten mit digital hinterlegten Informationen verhindern – mit direkten Auswirkungen auf den Betrieb und unter Umständen die Geschäftskontinuität betroffener Organisationen. Für Sabotageaktionen kommen beispielsweise Wiper-Werkzeuge zum Einsatz, die Geräte dauerhaft unbrauchbar machen.

Für April hat EuRepoC 29 dieser Operationen mit Störabsicht dokumentiert. Ein knappes Drittel davon entfiel auf DDoS-Angriffe, die bei erfolgreicher Durchführung für alle Nutzer:innen leicht und unabhängig von technischer Analyse zu beobachten sind. Trotz ihrer in der Regel vernachlässigbaren technischen Wirkung finden diese Operationen deshalb medial starke Beachtung, was die öffentliche Bedrohungswahrnehmung erhöhen, den psychologischen Effekt verstärken und darüber unter Umständen den Angreifern Vorschub leisten kann.

Anfang April wiesen Berichte über geleakte US-Geheimdienstdokumente auf Aktivitäten einer pro-russischen Hacktivistengruppe in den Netzen eines kanadisches Gasfernleitungsunternehmens hin. Danach soll die kriminelle Gruppierung Zarya in der Lage gewesen sein, den Ventildruck in Pipelineabschnitten zu erhöhen und Notabschaltungen auszulösen.

Mitglieder der Gruppe reklamierten die Fähigkeiten hierzu gegenüber Russlands Inlandsnachrichtendienst FSB. Angesichts des ständigen Wettstreits hacktivistischer Verbindungen um die Aufmerksamkeit staatlicher Stellen sind allerdings Überhöhungen tatsächlicher Mittel und Möglichkeiten nicht auszuschließen. Die an die Öffentlichkeit gelangten US-Geheimdienstberichte sprechen zumindest davon, dass FSB-Offiziere in Folge verstärkt kanadische Nachrichten in Hinblick auf Anzeichen für eine Explosion verfolgten, in der Erwartung, dass eine erfolgreiche Operation eine Detonation an einer Gasverteilerstation verursachen würde.

Der kanadische Premierminister Justin Trudeau schien den Vorfall im Rahmen einer Presseerklärung zu bestätigen, indem er Berichte über die Ereignisse einräumte, jedoch klar stellte, dass keine physischen Schäden an kanadischer Energieinfrastruktur infolge von Cyberangriffen zu verzeichnen seien.

Beobachtungen der Gruppe deuten darauf hin, dass die Bedrohungsakteure mehrere Tage auf weitere Anweisungen warteten, aber in erster Linie darauf abzielten, den Pipelinebetreiber finanziell zu verletzen, ohne die Infrastruktur selbst zu schädigen.

Zweifel bestehen über Zaryas Fähigkeiten, effektiv in den Betrieb einer Pipeline einzugreifen. Bei der Gruppierung handelt es sich um eine Abspaltung des Kollektivs Killnet, einer Verbindung, die vor allem durch DDoS-Angriffe gegen internationale Unterstützer der Ukraine in Erscheinung getreten ist. Störmaßnahmen gegen westliche kritische Infrastruktur, wie im Falle der kanadischen Pipeline, sind nichtstaatlichen pro-russischen Gruppen bisher nicht öffentlich zugeschrieben worden.

Kurz nach Bekanntwerden dieser Aktivitäten hatte die britische Regierung mit Nachdruck auf die von mit Russland sympathisierenden Gruppen ausgehende Gefahr aufmerksam gemacht. Ideologisch motiviert agierten diese Akteure opportunistisch mit dem unmittelbaren Ziel, Infrastruktur zu stören oder zerstören. Anders als nachrichtendienstliche oder militärische Kräfte, zeigten diese nichtstaatlichen Elemente wenig Zurückhaltung, seien zwar durch nationale Interessen angeleitet, stünden aber außerhalb staatlicher Kontrolle.

Der zweithäufigste im April verzeichnete Operationstyp waren „Hijacking with Misuse“-Operationen. Als Sammelbegriff fasst dies Aktionen, bei denen es Angreifern gelungen ist, in Systeme und Netzwerke einzudringen, um dort bereits unbefugt schädliche Aktionen auszuführen.

Diese Aktivitäten werden, sofern erkennbar, weiter nach ihrer Absicht differenziert und können Datendiebstahl oder Betriebsstörungen umfassen. Von diesen Aktionen hat EuRepoC 26 erfasst.

Beispielhaft dafür sind beharrliche Spionageunternehmungen der Gruppe Winter Vivern. Wie im letzten Monat im EuRepoC Cyberkonflikt-Briefing berichtet, reichen deren Operationen bis ins Jahr 2021 zurück und fallen in der Zielauswahl mit russischen und belarussischen Interessen zusammen. Ein in Folge des russischen Angriffskrieges verstärktes aufklärerisches Interesse an US-amerikanischen und europäischen Beratungen und Einschätzungen zum Kriegsverlauf schlägt sich auch in der Ausrichtung von Winter Vivern nieder. Charakteristisch sind dabei Bemühungen, Angriffstechniken auf einzelne Ziele zuzuschneiden, wie sich Anfang 2023 anhand der ausdifferenzierten Ausnutzung einer Schwachstelle in einer Software des Herstellers Zimbra beobachten ließ, die europäische Regierungen für eigene Webmail-Portale verwenden. Außerdem auffallend sind Anbahnungsversuche, bei denen die Gruppe anstrebt, sich als im Kontext des Kriegs gegen die Ukraine bekannt gewordene Expert:innen und andere Wissensträger:innen auszugeben, um sich so das gesteigerte Bedürfnis eines gemeinschaftlichen Informationsaustausches zu Angriffszwecken zunutze zu machen.

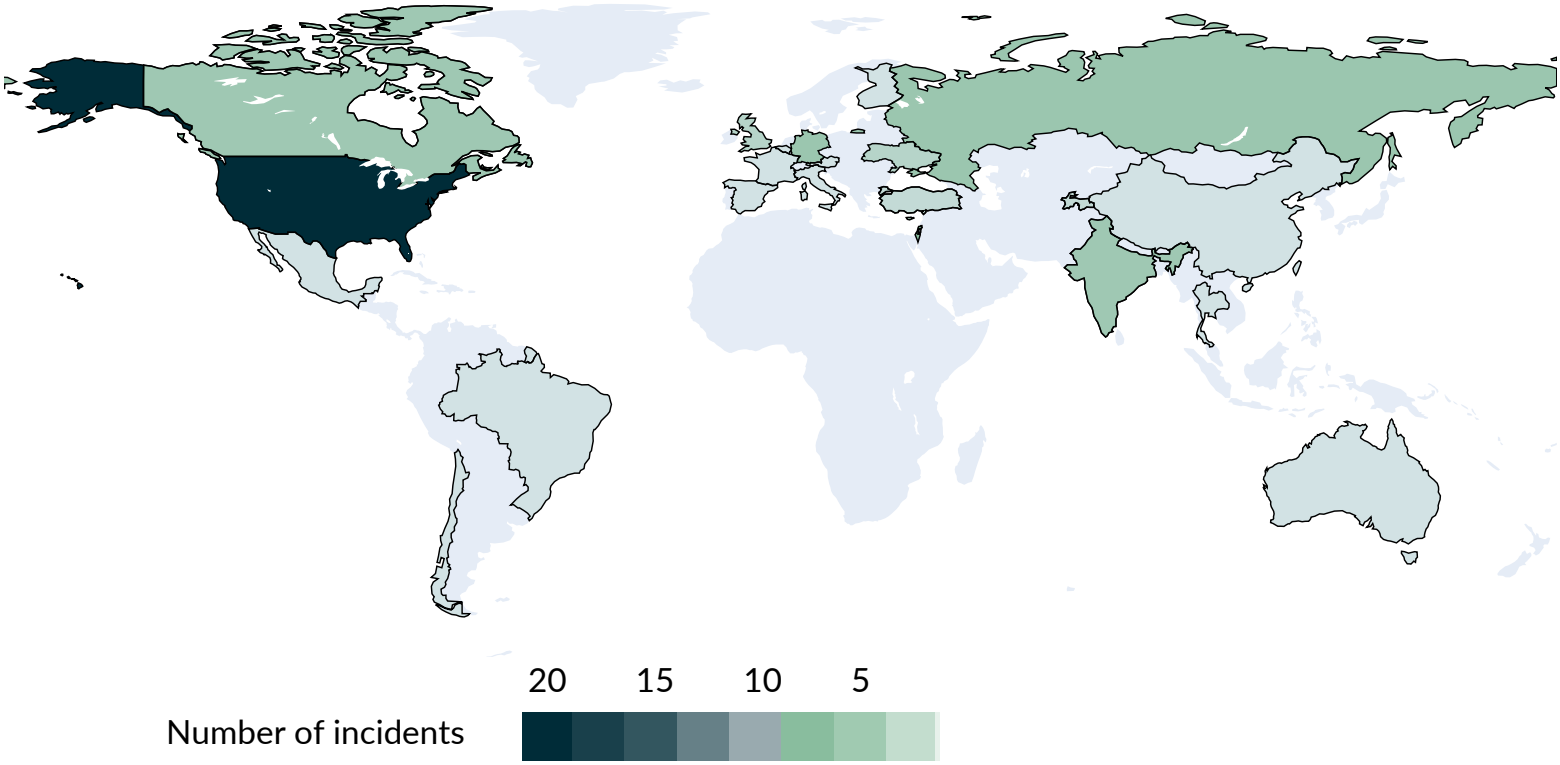
Unter anderem Angehörige der britischen Cybersicherheitsbehörde weisen in ihren Lagebeobachtungen darauf hin, dass Spionageoperationen – wie die von Winter Vivern – weiterhin eine große Unbekannte in der Bewertung darstellen, welche Rolle Cyberfähigkeiten für Russland in der Kriegsführung gegen die Ukraine eingenommen haben.

Brennpunkte und Zielmuster

Die für April erfassten betroffenen Länder verteilen sich mit fast zwei Dritteln der Vorfälle überwiegend auf Europa und Nordamerika. Das verbleibende Drittel betrifft vorrangig Fälle in Israel (sechs Vorfälle), nicht näher spezifizierte Staaten auf dem afrikanischen Kontinent (4) und Indien (2). Von den Vorfällen in Europa und Nordamerika waren die Vereinigten Staaten am häufigsten betroffen (18), gefolgt von Russland (5, wird zu Europa gezählt) und Deutschland (4). Die Russland betreffenden Vorfälle lassen sich dabei alle in den Kontext des andauernden Krieges gegen die Ukraine setzen.

Der im April 2023 am häufigsten betroffene Zielsektor waren Kritische Infrastrukturen mit 50 Fällen und einem Anteil von fast 80% aller aufgenommen Fälle, im Gegensatz zum Vormonat, in dem staatliche/politische Institutionen oder Akteure mit 67 Fällen am häufigsten anvisiert wurden. Hier fand ein Rückgang um 66% auf 22 Fälle statt. Dabei ergeben sich für die betroffenen Staaten im Einzelnen Unterschiede: So war in Nordamerika der am häufigsten betroffene Sektor das Gesundheitswesen mit Vorfällen in Krankenhäusern in mehreren US-Bundesstaaten und in Kanada. Diese Entwicklung ließ sich im vergangenen Monat ebenfalls für Europa beobachten, sodass ein konkreter geographischer Bezug nicht erkennbar ist, sondern vielmehr von einer konkreten Gefährdung des Sektors ausgegangen werden muss.

Geographic distribution of operations

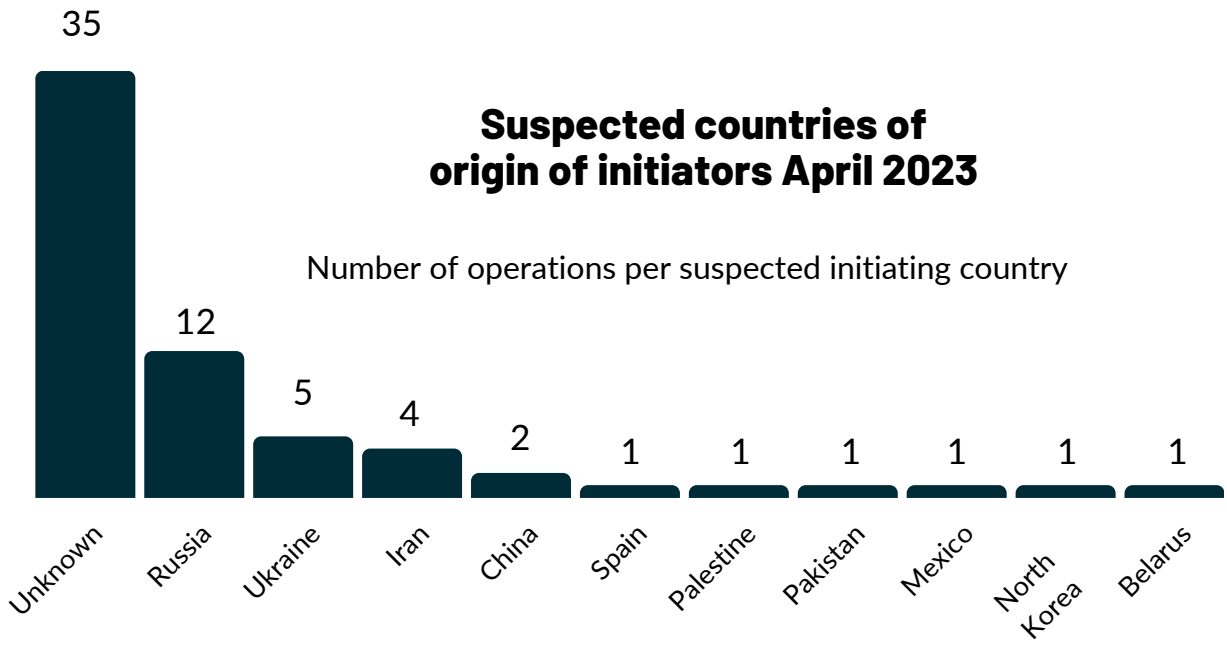


In Europa standen im April die Bereiche Transport und Maschinenbau mit jeweils zwei Vorfällen im Fokus, so etwa die Lürssen-Werft in Bremen. Andere Fälle mit Deutschland-Bezug betrafen DDoS-Attacken russischer "Hacktivisten" gegen die Webseiten von Polizeibehörden einzelner Bundesländer und die Entwendung von E-Mailzugangsdaten über die NATO School Oberammergau, die vermutlich mit der weiteren Unterstützung der Ukraine zusammenhängen.

In vielen Fällen ist die Urheberschaft von Angriffen nicht abschließend oder öffentlich geklärt. In einigen Fällen haben IT-Unternehmen bzw. Regierungen aber Hinweise auf die möglichen regionalen Ursprünge der Operation (aber nicht notwendigerweise auf staatliche Verantwortlichkeit) veröffentlicht.

Angreiferprofile und Attributionen

Auch im April 2023 dominierten auf Seiten der Angreifer Operationen, die russischen Akteuren zugesprochen wurden. Direkt dahinter folgten Angreifer mit ukrainischem Ursprung, was ebenfalls auf die nach wie vor hohe Frequenz an Cybervorfällen, aber auch die starke mediale Präsenz des Krieges im Allgemeinen hindeutet. Nachdem im März noch keine Vorfälle für iranische Akteure verzeichnet wurden, waren es im April nun vier Operationen mit attribuierter iranischer Herkunft. Im Vergleich zum Vormonat (und auch dem sonstigen Aktivitätsniveau) fällt zudem die mit zwei Vorfällen niedrige Anzahl an Operationen mit vermuteter chinesischer Herkunft auf. Dies kann zum einen daran liegen, dass es weniger Vorfälle gab, die die EuRepoC-Inklusionskriterien erfüllt haben.



Ein weiterer Grund könnte sein, dass die oftmals auf längerfristige (unentdeckte) Präsenz in den kompromittierten Systemen ausgelegten chinesischen Spionage-Operationen erst zu einem späteren Zeitpunkt entdeckt werden, etwa im Rahmen von Threat Intelligence Berichten. Neben den attribuierten Operationen führen jedoch auch im April wieder solche Operationen die Liste an, die (noch) keinem konkreten Land oder gar Akteur zugesprochen werden konnten, mit 55,6% der Fälle (35).

Im April stachen fünf Operationen heraus, die der Gruppierung “Anonymous Sudan” zugesprochen, beziehungsweise von dieser Gruppierung selbst für sich reklamiert wurden. Der genaue Hintergrund der Gruppe ist nach wie vor umstritten: Während manche Beobachter aus der Threat-Intelligence-Branche mittlerweile von einer russischen “False-Flag-Operation” ausgehen, sprechen andere Umstände für eine mögliche Eingliederung der zumindest offiziell islamisch-geprägten Gruppierung in die russische Hacktivisten-Gruppierung Killnet, nachdem Anonymous Sudan (aufgrund einer Koran-Verbrennung) mit Schweden und Dänemark pro-ukrainische Länder ab Mitte Februar attackierte.

Mehr Klarheit scheint darüber zu herrschen, dass die Gruppierung nichts mit der ursprünglichen “Anonymous Sudan” Gruppe zu tun hat, die sich 2019 im Zuge des Militärcoups im Sudan formiert hatte. Dass vier der fünf im April zur Datenbank hinzugefügten Operationen israelische Ziele anvisierten, könnte als Indiz für die nach wie vor pro-islamische Haltung der Gruppe, trotz öffentlicher Solidaritätsbekundungen gegenüber Russland, gewertet werden. Andererseits könnten auch Cyber-Operationen gegen Israel sowohl pro-islamisch/palästinensischen, als auch pro-russischen Zielen entsprechen, nachdem das Land im März die Lieferung von elektronischen Systemen zur Drohnenabwehr an die Ukraine bewilligt hatte. Ukraine-unterstützende Staaten, die sich den Zorn der islamisch-geprägten Hacker-Community zuziehen, könnten somit auch künftig ein attraktives Ziel für Anonymous Sudan/Killnet darstellen, um die angestrebte Verschleierung der eigenen Identität aufrecht zu erhalten.

Auch im Falle der am 7. April von Microsoft öffentlich gemachten Operation der iranischen staatlich-gesponserten Hacker-Gruppierung “Mango Sandstorm” (ehemals “MERCURY”, auch bekannt als “MuddyWater”) spielt die intendierte Verschleierung der eigenen Identität eine Rolle: Nachdem Mango Sandstorm den Zugang zu nicht näher beschriebener lokal installierter Software (“on-premises”) ermöglichte und an die iranische Gruppierung Storm-1084 (ehemals DEV-1084) weiter reichte, führte diese (manchmal erst nach monatelanger Erkundung der Netzwerke) disruptive Operationen darin durch, die auch die Cloud-Umgebung betrafen. So kam es zur “Zerstörung” verschiedenster Ressourcen, wie Server Farms, Virtual Machines, Storage Accounts und Virtual Networks. Laut Microsoft präsentiert sich Storm-1084 als angeblich finanziell motivierter Akteur, mutmaßlich um die eigentliche Verbindung zu staatlichen Stellen des Irans, wie etwa dem Ministry of Intelligence and Security (MOIS), welches vom US Cyber Command mit Mango Sandstorm assoziiert wurde, zu verschleiern.

Im April 2023 wurden zudem 15 Cybervorfälle und (somit nochmal 6 mehr als im Vormonat) dem konventionellen Konflikt zwischen Russland und der Ukraine zugeordnet, was das nach wie vor hohe Aktivitätsniveau sowohl pro-ukrainischer, als auch pro-russischer Hacker unterstreicht. So attackierte am 4. April die pro-russische Gruppierung NoName057(16) die Webseiten des finnischen Parlaments sowie der (früheren) Ministerpräsidentin Sanna Marin mit DDoS-Operationen, im Zuge des NATO-Beitritts des skandinavischen Landes.

Zusätzlich zu diesen technisch eher weniger anspruchsvollen und zumeist auch mit geringen Auswirkungen versehenen Hacktivisten-Operationen, verkündete die polnische Regierung am 13. April, dass der militärische Spionageabwehrdienst und das nationale CERT gemeinsam eine Spionageoperation der russischen APT29 (aka Cozy Bear) aufgedeckt haben. Diese begann bereits im Oktober 2022 und richtete sich gegen Außenministerien und diplomatische Entitäten von NATO- und EU-Ländern (sowie zu einem geringerem Maße auch afrikanischen Ländern). Bemerkenswert ist, dass die Stellungnahme die Motivation zur Veröffentlichung der Informationen transparent macht, nämlich *“to disrupt the ongoing espionage campaign, impose additional cost of operations against allied nations and enable the detection, analysis and tracking of the activity by affected parties and the wider cyber security industry.”*

Cyberspionage der profilierten russischen APTs ist somit nach wie vor ein wichtiges Mittel des Kreml, um die eigene Kriegsstrategie zu formen sowie übergeordnete (geo-)politische Entscheidungen zu treffen.

Dass gerade der Telekommunikationssektor in afrikanischen Ländern immer wieder (sieben Vorfälle im Datensatz) zum Ziel ausländischer Cyberspionage wird, demonstrierte zudem der Bericht des Threat Intelligence Unternehmens Symantec vom 20. April, in dem eine Spionageoperation der chinesisch-sprachigen APT “Daggerfly” (aka “Evasive Panda”), beginnend im November 2022 beschrieben wurde.

In demselben Bericht machte Symantec zudem die offensichtliche Weiterführung der Spionageoperation “Tainted Love” bekannt, die das Unternehmen SentinelOne im März offengelegt hatte. Dabei wurde die ebenfalls mutmaßlich chinesische APT “Othorene” (aka “Gallium”) für Operationen gegen Telekommunikationsunternehmen in Afrika und dem Nahen Osten (jedoch nur mit “moderate confidence”) verantwortlich gemacht, ebenfalls seit November 2022. Die geringere Sicherheit, mit der diese Attributionsaussage versehen wurde, spiegelt das hohe Maß an “TTP-sharing/diffusion” chinesischer Gruppierungen wider (TTP = *Tactics, Techniques and Procedures*), was eine zweifelsfreie Zuordnung von Verantwortlichkeiten zu einzelnen Gruppierungen erschwert. Telekommunikationsunternehmen stellen (besonders aufgrund wirtschaftlicher Interessen in diesem afrikanischen Sektor) nicht nur ein attraktives Primärziel für Spionage dar, sondern können auch als hilfreiches Einfallstor fungieren, um (z.B. über Supply-Chain-Operationen) an Informationen eigentlich anvisierter Endkunden zu gelangen.

Mehr von EuRepoC

Vom 11. bis 12. Mai veranstaltete EuRepoC mit externen TeilnehmerInnen aus Politik, Wissenschaft und der Threat Intelligence Branche in Innsbruck einen interdisziplinären Workshop mit dem Titel *“New Threats, New Methods, New Norms: Current Developments in Cybersecurity Theory and Law”*. Dabei wurden in unterschiedlichen Sessions aktuelle Angreifertrends (in der Ukraine und darüber hinaus), der Stand eines potenziellen europäischen Attributionsprozesses, sowie erste Befunde basierend auf der EuRepoC-Datenbank zu den völkerrechtlichen und technischen Kategorisierungen präsentiert und diskutiert.

Zudem erschien am 25. Mai ein weiteres APT-Profil zur russisch/belarussischen Gruppierung UNC1151, die unter anderem für die Ghostwriter-Kampagne verantwortlich gemacht wird und sich durch die Verbindung von Hacking und Desinformations-Taktiken auszeichnet.

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

Kerstin Zettl-Schabath ist Wissenschafterlin 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


@EuRepoC


linkedin/EuRepoC


contact@eurepoc.eu


https://eurepoc.eu