European
Repository of
Cyber Incidents

EuRepoC

Cyber Conflict Briefing

Juli 2023

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

Beobachtungen zur Gesamtlage

Im **Juli 2023** wurden 52 Cyber-Operationen in die EuRepoC-Datenbank aufgenommen. Das sind 31% weniger als im Vormonat, und 1 Operation weniger als die insgesamt durchschnittlich verzeichnete Aktivität von 53 Cyber-Operationen pro Monat im Gesamtzeitraum. Verantwortlich für diesen Rückgang könnte vor allem auch die aktuelle Sommerzeit sein, denn auch staatliche Hacker und Cyberkriminelle gehen in Urlaub, sodass im Juli und August üblicherweise weniger Aktivitäten erfasst werden.

Die **durchschnittliche Intensität** der im Juli 2023 erfassten Operationen beträgt 2,84 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

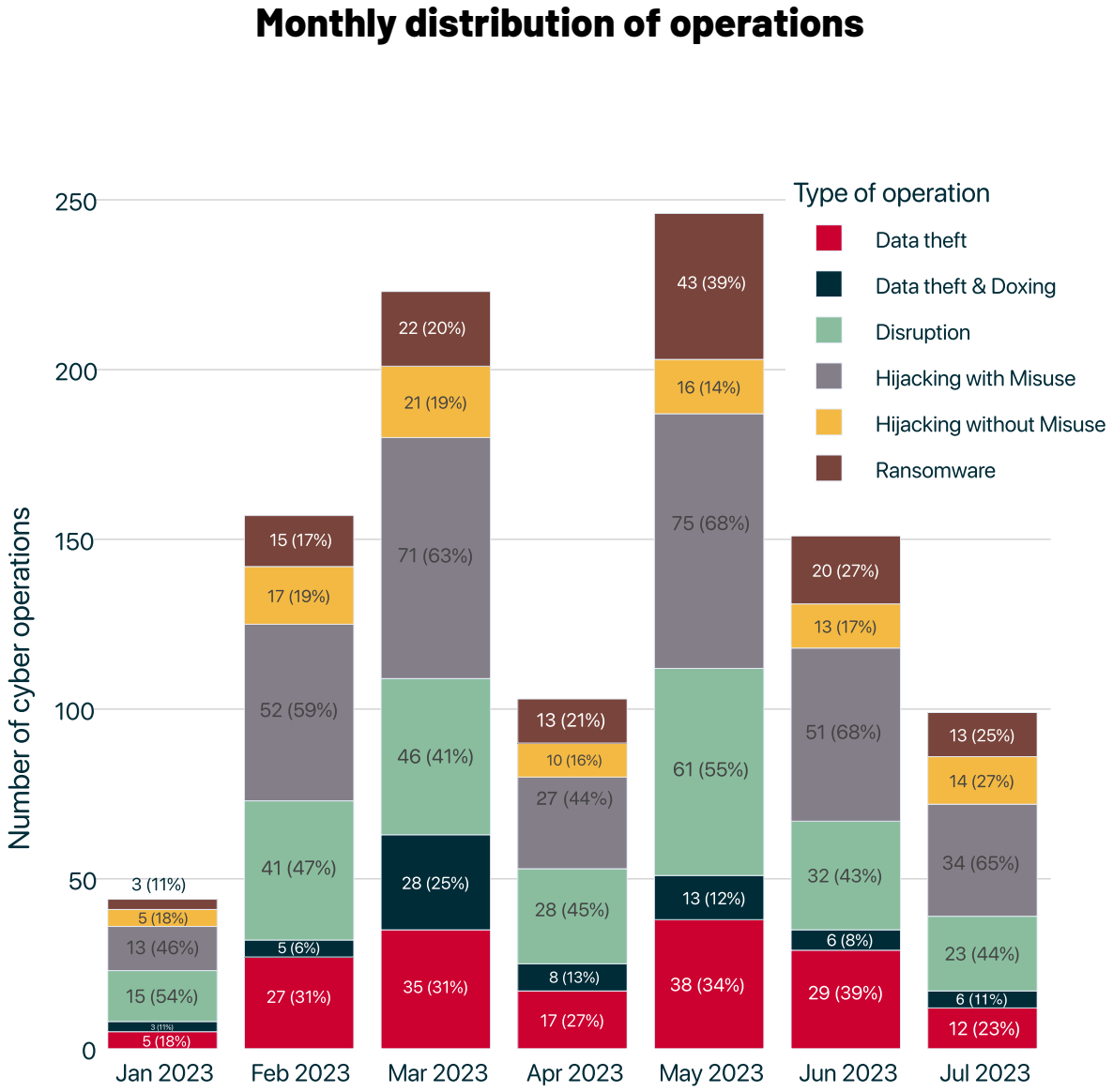
Analysen für das Cyber Conflict Briefing werden von EuRepoC erstellt. Die deutsche Ausgabe wird in Zusammenarbeit mit dem **Tagesspiegel Cybersecurity Background** veröffentlicht.
Das Briefing fasst die zentralen Trends, Dynamiken und Befunde zu den von EuRepoC in einem bestimmten Monat erfassten Cybervorfällen zusammen. Diese müssen nicht notwendigerweise im Juli 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 Juli 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 (65%). 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.

Von besonderer Tragweite war eine Mitte Juli von Microsoft eingeräumte chinesische Spionage-Kampagne der Gruppe Storm-0558, die nach Medienberichten in den USA mindestens mehrere hunderttausend Regierungsnachrichten erbeutete. Schlagzeilen machte, dass auch E-Mail-Accounts der US-Handelsministerin, des US-Botschafters in China und des Unterabteilungsleiters für Ostasien im State Department betroffen waren. Erste Analysen von Microsoft wiesen darauf hin, dass sich Storm-0558 in vergangenen Ausspähversuchen ebenfalls auf europäische Ziele konzentriert hatte.

Zwischenzeitlich haben weiterführende Untersuchungen unabhängiger Sicherheitsfirmen, unter anderem des Cloudsicherheitsunternehmens Wiz, ein weitaus umfassenderes Gefährdungspotential ermittelt.

Storm-0558 gelang der Zugriff auf durch Microsoft verwaltete E-Mail Konten über einen gestohlenen Signaturschlüssel für Microsoft Account (MSA), ein Dienst, über den der Softwareanbieter Zugriffsberechtigungen überprüft. Mithilfe des Schlüssels waren die Bedrohungsakteure in der Lage, selbstständig Zugangstoken zu erstellen, die uneingeschränkten Zugriff selbst auf Konten mit aktivierter Multifaktorauthentifizierung gewährten. Obwohl der Schlüssel eigentlich für Verbraucherkonten ausgelegt war, ermöglichte ein Fehler in der Gültigkeitsprüfung auch die Ausfertigung von Token für den an Geschäftskunden gerichteten Identitätsdienst Azure Active Directory (Azure AD). Microsoft selbst bewirbt Azure AD als Zugriffsschutz, „um 99,9 Prozent der Cybersecurity-Angriffe abzuwehren“. Auf diesem Weg erreichten die Angreifer auch die Accounts von Regierungsbehörden. Über diesen Anschluss an Azure AD konnten mit dem gestohlenen Schlüssel darüber hinaus Zugangstoken für eine Vielzahl weiterer Microsoft-Cloud-Dienste erzeugt werden. Um einer Ausnutzung entgegenzuwirken, sperrte Microsoft den betroffenen Schlüssel und hob damit verbundene Tokens auf. Neu angefertigte Schlüssel werden nun auch für Verbraucherkonten in einer verstärkt gesicherten Hardwareumgebung hinterlegt.

Nach Erkenntnissen von Wiz könnten Anwendungen, die Zugriffsberechtigungen anhand lokal gespeicherter Zugangsdaten bestätigen, weiterhin anfällig für die gefälschten Tokens sein. Da Logs im Vorfeld des Falles nur in bestimmten Bezahlmodellen zur Verfügung standen, ist es App-Entwicklern mitunter nicht möglich, eine eventuelle Kompromittierung nachzuvollziehen. Microsoft hat seitdem angekündigt, Zugriffsprotokolle frei zugänglich zu machen. Nachträglich kann diese Umstellung allerdings keinen Aufschluss geben. Das gesamte Ausmaß ist daher in seiner Wirkung praktisch fast nicht zu erfassen.

Die nach Bekanntwerden des Falls ergriffenen Maßnahmen sind in ihren Schutzmöglichkeiten in zweierlei Hinsicht begrenzt. Zum einen haben Bedrohungsakteure womöglich Hintertüren in den Zielumgebungen eingerichtet und sich insoweit vom kompromittierten und nun gesperrten Schlüssel unabhängig gemacht. Zum anderen beeinflusst, wie der Sicherheitsforscher und frühere NSA-Mitarbeiter Jake Williams festhält, die Offenlegung der Kompromittierung die Operationslogik der Angreifer. Die ursprünglich selektive Zielauswahl von Storm-0558 war dadurch motiviert, möglichst lange unentdeckt zu bleiben. Die Aufdeckung der Spionagekampagne führt zu einer Umkehr dieser Anreizstruktur, nach der die maximal mögliche Ausnutzung von Anwendungen, die aktuell noch über die „Log in with Microsoft“-Funktion anfällig sind, an Bedeutung gewinnt.

Am 11. August gab der US-Heimatschutzminister bekannt, dass sich das Cyber Safety Review Board in seiner bisher erst dritten Untersuchung mit dem Fall beschäftigen und Empfehlungen erarbeiten wird.

Der zweithäufigste im Juli 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 23 davon erfasst.

Anhaltend hohe Ransomware-Aktivität bestimmt weiterhin das Muster disruptiver Operationen, auch wenn nach Erhebungen des Forensikunternehmens Coveware der Anteil betroffener Organisationen, die Lösegeldforderungen erfüllen, im zweiten Quartal 2023 mit 34% einen Tiefstand erreichte. Vier Jahre zuvor lag dieser Wert noch bei fast 80%. Dieser Rückgang wird in Teilen durch einen massiven Anstieg der Höhe der geleisteten Lösegeldzahlungen relativiert. Im zweiten Quartal belief sich die durchschnittliche Summe dieser Zahlungen auf mehr als $740.000 – eine Steigerung von 126% im Vergleich zum vorangegangenen Quartal.

Ziel eines solchen Erpressungsversuches war auch die Bangladesh Agricultural Bank (BKB), wie die verantwortliche Ransomware-Gruppe AlphV/BlackCat am 7. Juli bekannt gab. Vertreter der Bank hatten zuvor bestätigt, dass Hacker Zugang zu Servern erlangt hatten. Bangladeschische Medien berichteten unter Berufung auf Angaben von Bankangestellten Probleme mit dem Zugang zu Softwaresystemen.

Laut Einschätzungen der Bank sei es im Rahmen des Vorfalls nicht zum Abfluss von Daten oder der Unterbrechung von Kundendienstleistungen gekommen. Spätere Aussagen des geschäftsführenden Direktors der Bank versuchten die Ereignisse in einen anderen Zusammenhang zu setzen, dementierten einen Hack und machten Serverwartungen für den Zwischenfall verantwortlich.

Diese Aussagen nach dem Vorfall weichen von früheren Auskünften der Bank ab, wonach externe Störungen auch zeitweise Banktransaktionen beeinträchtigt hätten. Der Fall zeigt allerdings auch, dass die öffentliche Kommunikation von Ransomware-Opfern neben Transparenz und Zuverlässigkeit ebenfalls auf Einwirkungsversuche von Ransomware-Akteuren vorbereitet sein muss.

So standen die Managementäußerungen nicht nur im Kontrast zu von AlphV/BlackCat behaupteten Aktionen. Nachdem sich die Bank gegen Verhandlungen mit der Gruppe entschieden hatte, begann AlphV/BlackCat damit, mutmaßlich gestohlene Daten zu veröffentlichen und vorherige Aussagen der Bank zu Art und Ausmaß des Vorfalls in Zweifel zu ziehen. In Androhung einer weiteren Eskalationsstufe verkündete die Gruppe die Absicht, sich mit erbeuteten Kontaktdaten direkt an BKB-Kunden zu wenden.

AlphV/BlackCat stellte in Aussicht, Kunden in einer fingierten Warnung über die drohende Zahlungsunfähigkeit der Bank zum Abziehen ihrer Einlagen zu bewegen. In kritischer und konzentrierter Masse könnten solche Kapitalabzüge auch das Potential für einen Bank-Run entwickeln.

Die Abwendung eines solchen Szenarios hängt zu wesentlichen Teilen auch vom Vertrauensverhältnis des betroffenen Unternehmens zu den eigenen Kunden ab – eine Umsetzungsvariable in Incident-Response-Plänen, die Unternehmen üblicherweise stärker kontrollieren können.

AlphV/BlackCat stellte im Juli zudem der breiteren Öffentlichkeit eine "Application Programming Interface" (API) für ihre Erpressungs-Website zur Verfügung, mutmaßlich um noch mehr Druck auf die Opfer auszuüben, die zuletzt häufiger von Lösegeldzahlungen abgesehen hatten, wie z.B. das US-Kosmetik-Unternehmen Estée Lauder.

Vergangene Aktionen der aus einer Abspaltung der für den Angriff auf Colonial Pipeline verantwortlichen Ransomware-Gruppe DarkSide hervorgegangenen Bande zeigen, dass Mitglieder auch zu Aktionen bereit sind, die längerfristigen wirtschaftlichen Schaden verursachen.

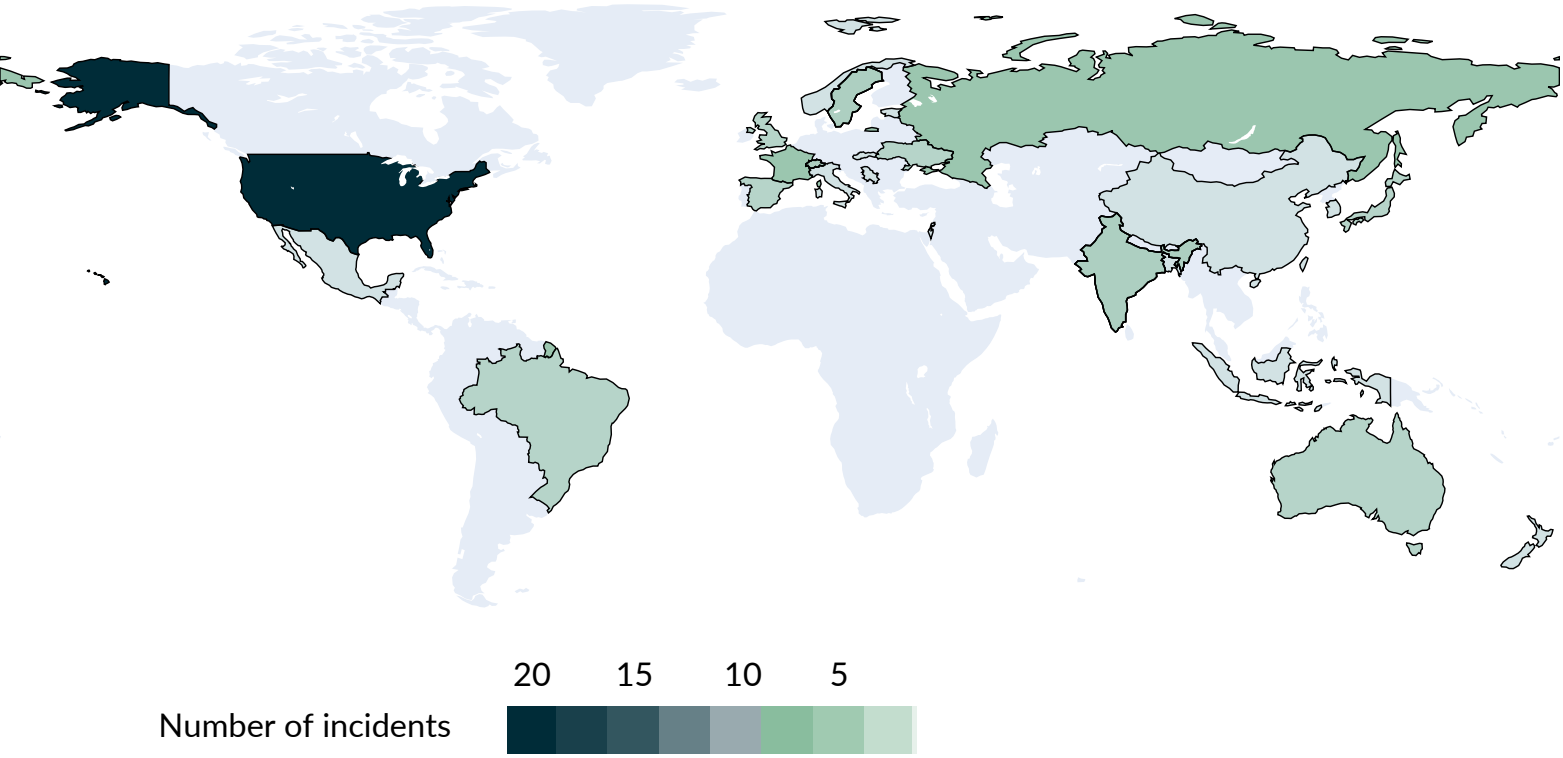
Brennpunkte und Zielmuster

Der am häufigsten im Juli 2023 betroffene Zielsektor war, wie auch schon im Vormonat, Unternehmen der Kritischen Infrastruktur mit 31 Fällen beziehungsweise 62% der neu aufgenommenen Fälle. Dies stellt einen Rückgang um etwa ein Drittel gegenüber der Anzahl an Fällen im Vormonat dar (45 Fälle), entspricht aber relativ einer gleichen Menge zum Vormonat. Am zweithäufigsten betroffen waren in 19 Fällen (38%) staatliche Institutionen, hier ergab sich gleichlaufend zum - sommerlichen - Gesamttrend ein Rückgang um 42%.

Die Vereinigten Staaten bleiben angesichts technischer und industrieller Exponiertheit am häufigsten von Cybervorfällen betroffen: Im Juli waren dies 18 Vorfälle, was in etwa der in den Vormonaten wahrgenommenen Menge von einem Drittel aller Vorfälle entspricht. Europäische Staaten waren insgesamt 20-mal (fast 40%) unter den Zielen von Cybervorfällen. Davon waren etwas mehr als die Hälfte Mitgliedstaaten der EU (10 Fälle), wobei in diesem Monat Frankreich mit vier Vorfällen am häufigsten betroffen war. Die Verteilung der Nicht-EU-Mitgliedsstaaten betraf Russland (4), Großbritannien (3), die Ukraine (3) sowie Norwegen und Serbien (je ein Vorfall). Für Deutschland wurde im Juli kein Vorfall in die Datenbank aufgenommen, was im Vergleich zu den Vormonaten eine auffällige Veränderung darstellt.

Innerhalb der Kritischen Infrastrukturen zeigt sich für Juli gegenüber den Vormonaten ein weiterer Ausreißer: Mit knapp einem Fünftel der Gesamtvorfälle (9) war der Finanzbereich die am häufigsten betroffene Branche. Dies betraf in der Mehrzahl "Diebstähle" auf Kryptowährungsbörsen, teils mit beachtlichen öffentlich bekannt gewordenen Schadenssummen, so etwa bei CoinsPad aus Estland mit einem gemeldeten Schaden in Höhe von 37,3 Mio. US-Dollar. Etwas niedriger fiel die Summe bei Poly Network aus, das bereits im Jahr 2021 betroffen gewesen war. Dass hiervon auch das klassische Finanzgeschäft nicht ausgenommen ist, zeigt der im vergangenen Jahr geschehene Diebstahl über 20 Mio. US-Dollar bei der britischen Neobank Revolut, der erst jetzt öffentlich wurde.

Geographic distribution of operations

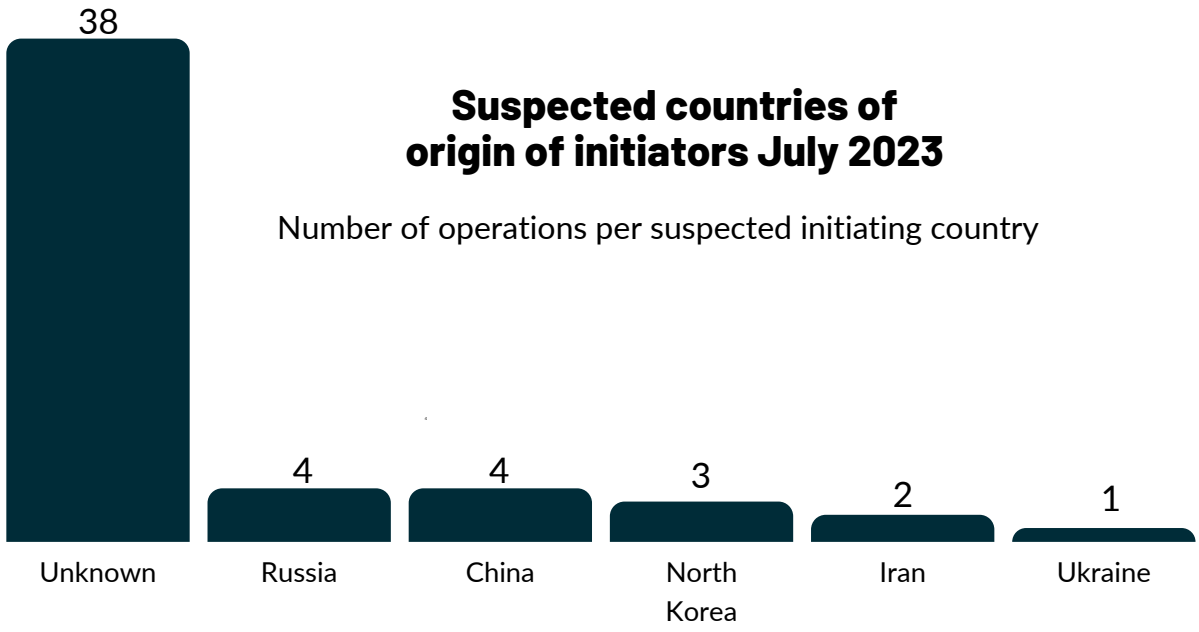


Weiterhin häufig betroffen bleibt unter den Betrieben der Kritischen Infrastruktur der Gesundheitssektor mit neun Fällen, eine Parallele zu den Vormonaten. Dabei handelte es sich im Juli in knapp der Hälfte der Fälle um Ransomware-Vorfälle, in zwei Dritteln kam es (auch) zum Diebstahl von Daten, die fast immer als sensibel klassifiziert werden konnten.

Bei staatlichen Institutionen zeigt sich mit elf Fällen eine hohe Anzahl an Operationen, die regionale und lokale Behörden anvisierten, so etwa zwei der vier Frankreich betreffenden Vorfälle. Wie bereits im Briefing für den Mai erwähnt, weisen regionale/lokale Behörden oftmals ein vermutlich niedrigeres IT-Sicherheitsniveau auf als nationale Behörden, für welche im Juli insgesamt sieben Fälle aufgenommen wurden. Regionale/lokale Behörden könnten daher vor allem auch zum Opfer sogenannter “Spray-and-Pray”-Aktionen werden, bei denen keine bestimmten Behörden zielgerichtet ins Visier genommen werden, sondern der Erfolg der Operation durch die hohe Anzahl an Infektionsversuchen gegen eine breite Masse an Organisationen sichergestellt werden soll.

Angreiferprofile und Attributionen

Auch im Juli pendelte sich der Prozentsatz der (noch) nicht konkreten Angreiferländern zugeordneten Cybervorfälle (Anzahl: 38) mit 73% auf ca. 70% der erfassten Operationen ein. In 20 der 52 Fälle wurden nichtstaatliche Akteure verantwortlich gemacht, das sind mit 38% lediglich ein Prozent weniger als im Vormonat Juni. Sogenannte "Cyber Proxies", also staatlich unterstützte und/oder beauftragte Hacking-Gruppierungen, wurden in acht Vorfällen als Täter identifiziert. Wie bereits zuvor im Monat Juni rangieren russische Cyberangreifer auch im Juli auf dem zweiten Platz, gemeinsam mit chinesischen Gruppierungen.



Suspected countries of origin of initiators July 2023

Number of operations per suspected initiating country

Auffällig ist im Juli die weitaus geringere Diversität erfasster Angreiferherkunftsländer. Außer den “üblichen vier Verdächtigen”, Russland, China, Iran und Nordkorea, findet sich lediglich die Ukraine in der Liste. Wie zuvor bereits für die allgemein deutlich geringere Fallanzahl im Juli diskutiert, kann auch hierfür zumindest in Teilen die “Sommerpause” offensiv agierender Akteure im Cyberspace verantwortlich gemacht werden. Dies könnte gerade für Länder relevant sein, die im Vergleich zu den genannten vier Ländern im Rest des Jahres bereits ein niedrigeres Aktivitätsniveau verzeichnen, was bei diesen somit zu einem gänzlichen Fehlen in unseren erfassten Vorfällen geführt haben könnte. Akteure aus Russland, China, Iran und Nordkorea sind stattdessen in weitaus höherer Anzahl und Frequenz offensiv im Cyberspace aktiv. Diese Länder verfügen zudem über eine historisch gewachsen größere Anzahl an patriotischen Hackergruppierungen sowie staatlich unterstützen APTs, weshalb selbst bei einer zeitweiligen Inaktivität der einen Gruppierung dennoch Vorfälle aus diesen Ländern auch in den Sommermonaten verzeichnet werden.

Aber auch auf Seiten der anvisierten Ziele sowie deren IT-Abteilungen, sowie auch den “abwehrenden” oder zumindest untersuchenden Incident Response/Threat Intelligence Unternehmen, könnte die Urlaubszeit im Juli und August zu einer geringeren Kapazität zur Entdeckung, Analyse von sowie öffentlicher Berichterstattung über Cyberangriffe führen.

In sieben der acht Vorfälle, in denen Cyber Proxies als verantwortliche Akteure identifiziert wurden, wurde ebenfalls ein konkretes Land als Auftraggeber/Unterstützer genannt. Im Falle der 20 rein nichtstaatlichen Angreifern zugesprochenen Operationen wurde lediglich sechsmal ein Herkunftsland attribuiert. Von den übrigen 14 Operationen, die keinem Land zugeordnet wurden, waren sieben Ransomware-Operationen, für die oftmals kein spezifisches Land attribuiert werden kann, etwa weil die Gruppierung transnational agiert, wie eine Art international operierendes Cyber-Crime-Unternehmen. Weniger patriotische/nationale Motivlagen als vielmehr das gemeinsame Streben nach finanziellen Gewinnen ist hier der gemeinsame Nenner.

Dass dies jedoch im Falle eines gewaltsamen Konflikts wie des russischen Krieges gegen die Ukraine auch zu Unstimmigkeiten und Konflikten innerhalb einer transnationalen Cyber-Crime-Gruppierung führen kann, zeigten nicht zuletzt die sogenannten "Conti-Leaks" aus dem Vorjahr. Diese veranlassten andere Gruppierungen dazu, weder der Ukraine noch Russland öffentlich Unterstützung zu zusagen, sondern stattdessen politische Neutralität für sich zu reklamieren, um das eigene Geschäftsmodell nicht zu gefährden.

Des Weiteren wurden drei der 14 Fälle der Hacktivist-Gruppierung "SiegedSec" zugesprochen. Diese formierte sich öffentlichen Erkenntnissen nach im April 2022 und verübt nach eigenen Angaben zumeist politisch motivierte Angriffe, sieht sich selbst dennoch eher als "Black Hats" denn als Hacktivisten, da es ihren Mitgliedern oftmals einfach auch nur um Chaos und (digitale) Zerstörung gehe. Derlei Aussagen lassen sich häufig nur schwer beurteilen oder gar verifizieren. In einem Fall vom Juli hatte die Gruppierung mehr als 700 interne Dokumente des NATO Community of Interest Cooperation Portal gestohlen und am 24. Juli via Telegram veröffentlicht. Laut eigenen Angaben geschah dies nicht im Kontext des russischen Krieges gegen die Ukraine, sondern in Reaktion auf behauptete, nicht näher benannte "Human Rights Abuses" von NATO-Staaten. An dieser Stelle können keine weiterführenden Spekulationen über die Glaubwürdigkeit dieser Aussagen getätigt werden, auffällig ist bislang jedoch der starke Fokus der Gruppierung auf US-Ziele, wie etwa auch bei zwei weiteren Fällen, die im Juli in die EuRepoC-Datenbank aufgenommen wurden.

Im ersten Fall nahm die Gruppe verschiedene US-Bundesstaaten angeblich aufgrund ihrer jüngsten Gesetzesinitiativen zum Verbot von geschlechtsangleichender Behandlung für Transgender-Jugendliche ins Visier und stahl nach eigenen Angaben Daten und verunstaltete ("Defacement") deren Webseiten. Im zweiten Fall erlangte die Gruppe Zugang zu den Systemen des US-Technologie-Unternehmens ITC Global und löschte Kunden-Accounts, die zur Überwachung von Satelliten-Receivern genutzt werden. Darüber hinaus gab die Gruppe an, Satelliten-Receiver und Industrial Control Systems (ICSs) über mehrere US-Bundesstaaten hinweg "anvisiert" zu haben, ebenfalls aufgrund deren Gesetzesvorhaben zum Verbot von Geschlechtsangleichungen. Ob und in welcher Form die genannten Ziele tatsächlich von Cyberoperationen betroffen waren, blieb jedoch ungeklärt.
Das Beispiel von SiegedSec verdeutlicht die äußerst herausfordernde Zuschreibung von Angreifer-Identitäten auf Basis selbst kommunizierter Motivlagen, da diese über Fälle hinweg variieren, oder aber ein lediglicher Vorwand zur Verschleierung der eigentlichen Beweggründe sein können. Aufgrund der oftmals jedoch heterogenen Zusammensetzung und Mitgliederstruktur von Hacktivisten-Gruppierungen ist es dennoch prinzipiell möglich, dass deren Operationen über Zeit keinem stringenten Ziel- und Motivprofil folgen.

Die am 26. Juli durch die chinesische Zeitung Global Times öffentlich gemachte Cyberoperation gegen das Wuhan Earthquake Monitoring Center spiegelt die zeitweilige "Nachahmung" öffentlich-privater, in Teilen kooperativer oder arbeitsteilig ablaufender Attributionspraktiken westlicher Länder seitens der Volksrepublik wider. So haben dem Bericht zufolge sowohl das staatliche Computer Virus Emergency Response Center als auch das chinesische Cyber-Sicherheitsunternehmen 360 Security Technology einen nicht näher spezifizierten Trojaner in Netzwerktechnik des Centers gefunden, die für seismische Beobachtungen eingesetzt wird. Erste Untersuchungen machten der Global Times zufolge Angreifer mit staatlichem Hintergrund für den Vorfall verantwortlich. Des Weiteren sei die Aktivität auf das Gebiet der USA zurückgeführt worden. Offiziell stellt dies keine direkt-staatliche Attribution gegenüber den USA dar, da der Angriff aus technischer Sicht lediglich von Servern oder Computern in den USA hätte erfolgen, aber von einem anderen Land aus initiiert und gesteuert werden können. Nichtsdestotrotz dürfte mit dieser indirekten Attribution eine Signalfunktion gegenüber den USA durchaus gewollt gewesen sein.

Auch wenn im weiteren Verlauf des Medienberichts Äußerungen der Sprecherin des Außenministeriums erwähnt werden, die den USA u.a. Doppelstandards und eigene Cyberangriffe vorwerfen, kann nicht eindeutig bestätigt werden, dass sich diese berichteten Aussagen auf den vorliegenden Fall in Wuhan bezogen haben.

Dass neben Kaspersky und Group-IB auch noch weitere russische Unternehmen in das "Attribution-Business" eingestiegen sind, zeigt ein Bericht von Positive Technologies. Die Firma war im April 2021 vom US Finanzministerium für das Bereitstellen von Computer-Netzwerk-Sicherheitslösungen u.a. für den russischen Inlandsgeheimdienst FSB, sowie auch am 23. Juni 2023 von der EU im Rahmen der Verordnung Nr. 269/2014 sanktioniert worden. In dem Bericht vom 24. Juli 2023 macht das Unternehmen eine Cyberspionage-Operation chinesischer Cyber-Krimineller mit dem Namen "Space Pirates" gegen russische und serbische Organisationen öffentlich.

Mehr von EuRepoC

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

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

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

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