European
Repository of
Cyber Incidents

EuRepoC

Cyber Conflict Briefing

März 2024

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

Beobachtungen zur Gesamtlage

Im **März 2024** wurden 71 Cyber-Operationen in die EuRepoC-Datenbank aufgenommen. Das sind 33,6% weniger als im Vormonat. Insgesamt entspricht dieser Wert jedoch der durchschnittlich verzeichnete Aktivität von 71 Cyber-Operationen pro Monat im Gesamtzeitraum.

Die **durchschnittliche Intensität** der im März 2024 erfassten Operationen beträgt 2,42 und liegt somit unter dem historischen Durchschnitt (2,8). 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 März stattgefunden haben, sondern können bereits zu einem früheren Zeitpunkt begonnen haben. Dabei stehen technische, politische sowie rechtliche Aspekte im Vordergrund.

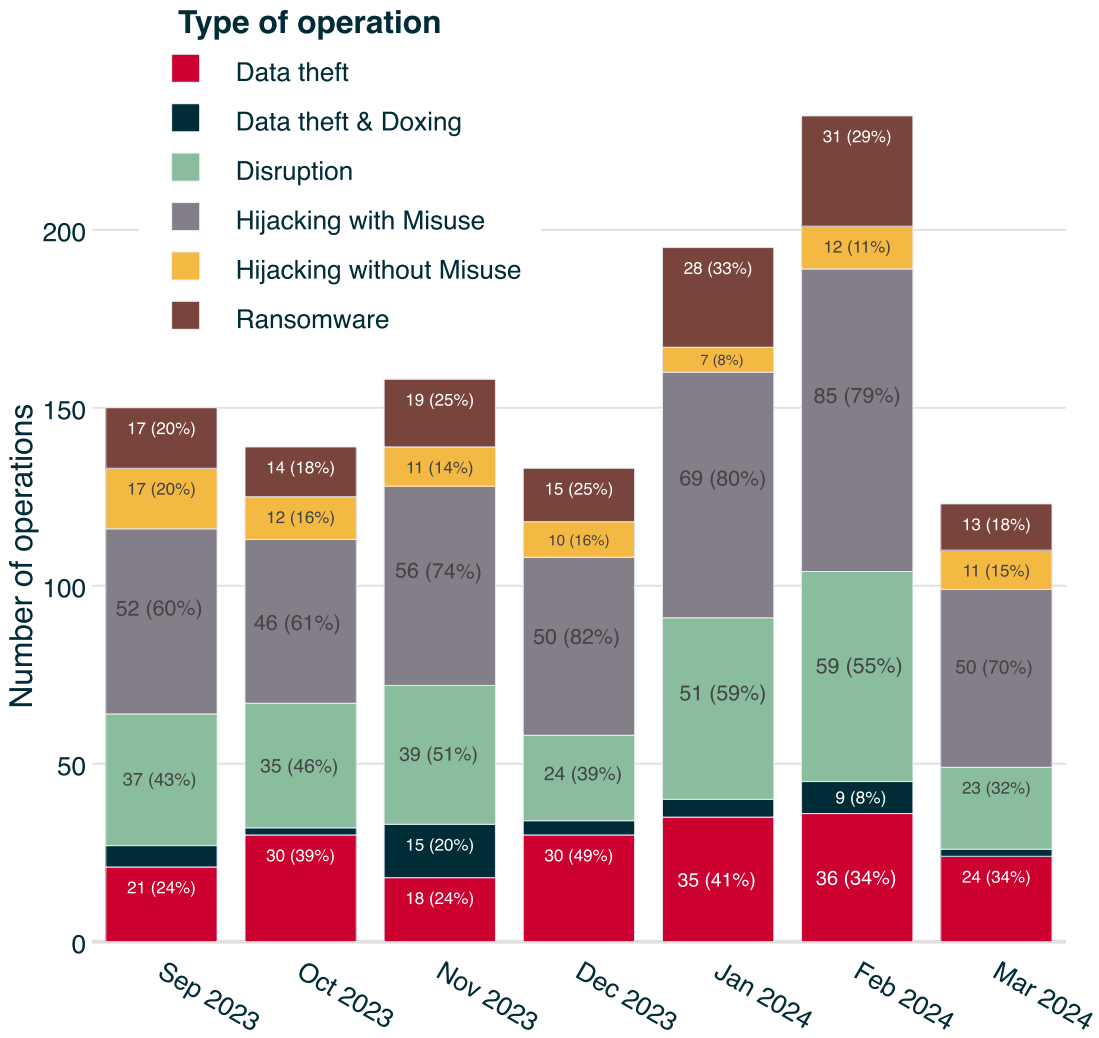
Über EuRepoC

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 März 2024 erfassten Vorfälle verteilen sich auf folgende **Operationstypen**:

Monthly distribution of operations



Hinweis: Einzelne Cybervorfälle können mehrere Operationstypen in Kombination aufweisen.

Der größte Anteil umfasst „Hijacking with Misuse"-Operationen mit 50 Fällen (70%). 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.

Die tschechische Cybersicherheitsfirma Avast etwa meldete einen sorgfältig geplanten Hijacking-Versuch der durch den nordkoreanischen Geheimdienst gesteuerten Lazarus Group. Dabei nutzte Lazarus eine besonders tiefgreifende, zuvor nicht bekannte Schwachstelle, um mithilfe eines systemeigenen Treibers von Windows Zugriff auf die Kernel-Ebene – den Kern des Betriebssystems, der als Schnittstelle zwischen Software und Hardware fungiert – zu erhalten. Der für die Operation genutzte Treiber unterstützt AppLocker, eine eingebaute Windows-Funktion, um bestimmte Softwareanwendungen für ein System freizuschalten.

Dieser Angriffspfad zielt direkt auf einen Baustein der Windows-Sicherheit ab, der für die Durchsetzung von Anwendungsrichtlinien verantwortlich ist. Die Ausnutzung dieser Zero-Day-Schwachstelle in einem integrierten Treiber ermöglichte es Lazarus, Kernel-Rechte zu erlangen und beliebigen Code auszuführen. Der darüber erweiterte Zugriff ermöglichte es der Gruppe, Sicherheitssoftware zu deaktivieren und Kernel-Objekte direkt zu manipulieren.

Im Gegensatz zu anderen Vorfällen, die sich dieser BYOVD-Technik (Bring Your Own Vulnerable Driver) bedienen, bei denen Software von Drittanbietern geladen werden muss, zielte Lazarus auf einen Treiber ab, der auf den Zielsystemen durch das Betriebssystem vorinstalliert war. Dieser Ansatz kombiniert BYOVD-Techniken mit einer "living-off-the-land"-Taktik, was eine Entdeckung zusätzlich erschwert.
Die Schwelle zur Durchführung solcher Operationen liegt allerdings hoch, da die Anzahl der in Betriebssystemen integrierten Treiber geringer und deren Codequalität gegenüber höher ist.

Um die Ausnutzung der Sicherheitslücke nachvollziehen zu können, entwickelte Avast einen Proof-of-Concept, den das Unternehmen im August 2023 an Microsoft übermittelte. Microsoft stellte daraufhin im Februar 2024 im Rahmen des monatlichen Update-Zyklus einen Patch bereit. Im Zuge der Behebung der Zero-Day-Schwachstelle, die dieses Rootkit ermöglicht, konstatierten Avast-Forscher, dass Lazarus dadurch wahrscheinlich eines seiner komplexesten Werkzeuge verloren hat und möglicherweise auf weniger gut getarnte BYOVD-Techniken zurückgreifen muss. Allerdings Avast gab keine Details über das Opfer des Angriffs bekannt oder wie erfolgreich die Operation vor ihrer Entdeckung war.

Am zweithäufigsten wurden im März 2024 'Data Theft'-Operationen beobachtet (34%). Von diesem Operationstyp sind für März 24 durch das Repositorium erfasst. Betroffen durch einen solchen Datendiebstahl war im März unter anderem Acer Philippines, eine Tochtergesellschaft des taiwanesischen Herstellers von Computerhardware und -elektronik. Der unbefugte Zugriff auf Unternehmensdaten ereignete sich bei einem Dienstleister der Firma, der für die Verwaltung von Mitarbeiterdaten zuständig war. Ein unter dem Pseudonym "ph1ns" agierender Nutzer verbreitete einen Auszug der gestohlenen Informationen anschließend über ein Hackerforum und bot den Datensatz frei zum Download an.

In diesem Forumsbeitrag bekannte sich ph1ns zu der mutmaßlich hacktivistischen Vereinigung #OpEDSA. In Anlehnung an die EDSA-Revolution von 1986, einer gewaltfreien Bewegung, die sich gegen die Diktatur von Ferdinand Marcos auflehnte und für die Wiedereinführung der Demokratie in den Philippinen einsetzte, beansprucht diese Gruppierung mit ihren Aktionen gegen autoritäre Strukturen und wirtschaftliche Missstände zu protestieren. In den Philippinen tätige Unternehmen stellen dabei für die Gruppe ein erklärtes Ziel dar, um Druck auf die politische Führung des Landes auszuüben.

Im konkreten Fall schloss der verantwortliche Akteur Verhandlungen mit Acer aus. Ph1ns gab an, selbst keine Erpressungsversuche gegen den Hersteller unternommen zu haben, und wies Belege für die Löschung von Daten auf angegriffenen Servern vor.

Dieses Vorgehen hebt die Risiken hervor, denen Unternehmen durch hacktivistische Aktivitäten in sozial- aufgeladenen Lagen ausgesetzt sein können. In dieser Hinsicht

weisen die Aktivitäten von #OpEDSA auch auf das disruptive Potential von hacktivistischen Manövern hin, in denen bewusst umkehrbare Aktionen, einschließlich der Verschlüsselung wichtiger Daten, mit bestimmten politischen Forderungen verbunden werden.

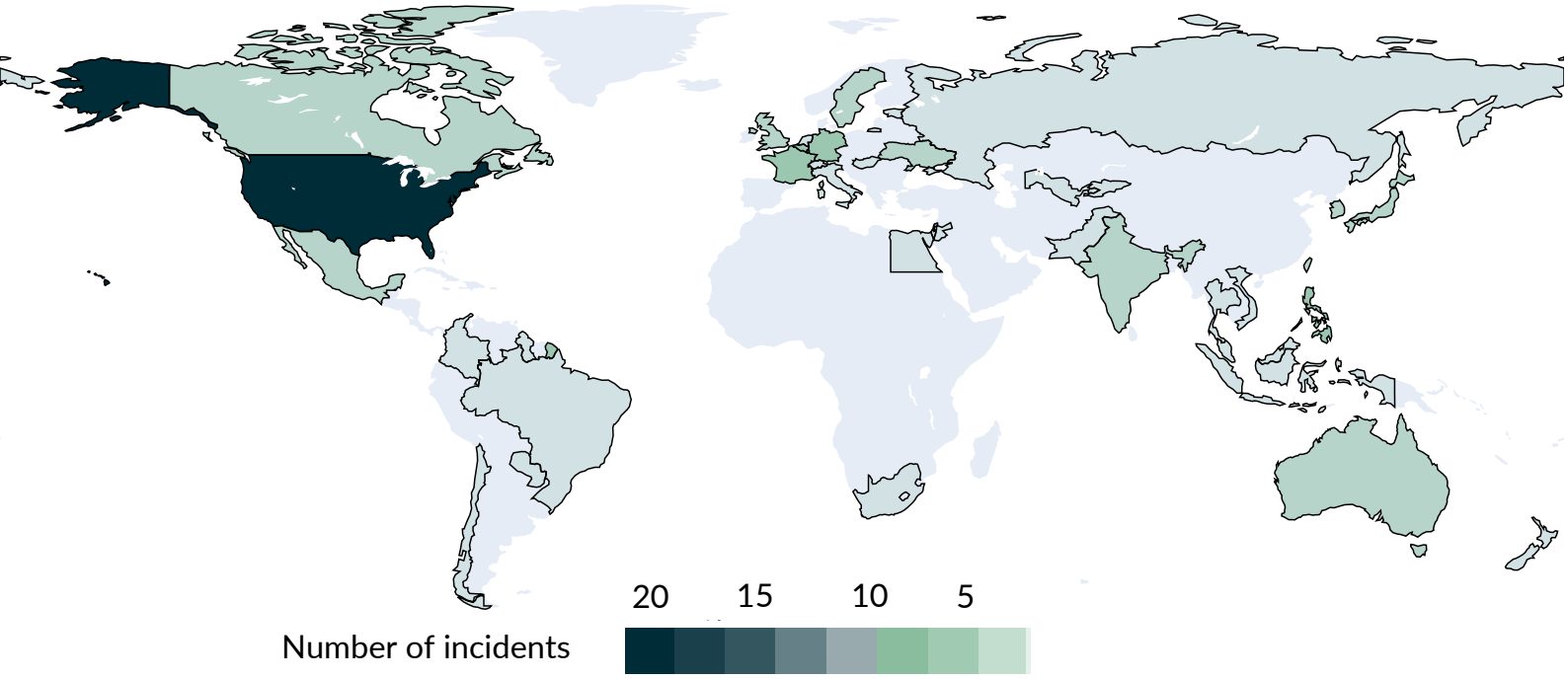
Brennpunkte und Zielmuster

Der am häufigsten im März 2024 betroffene Zielsektor waren staatliche Institutionen mit 36 Fällen, beziehungsweise 51% der neu aufgenommenen Fälle und lag damit erstmal seit dem Erscheinen des Briefings vor dem Bereich kritische Infrastrukturen, dem mit 33 Fällen in 46% aller Fälle betroffen war. Angesichts der geringeren Fallzahl gegenüber dem Februar handelt es sich um einen Rückgang der aufgenommenen Vorfälle um fast ein Viertel für staatliche Institutionen und sogar um ein Drittel für Unternehmen der kritischen Infrastruktur. Neben diesen beiden häufig betroffenen Sektoren waren in zehn Fällen (14% bezogen auf die Gesamtanzahl) Bildungseinrichtungen ebenso wie im Februar überproportional betroffen. Allerdings kann es hier je nach Organisation zu Doppelzählungen zwischen staatlichen Institutionen oder auch kritischer Infrastruktur kommen.

Am häufigsten betroffen waren erneut die Vereinigten Staaten mit 22 Vorfällen, ähnlich oft wie im Vormonat. Erneut verstärkt betroffen waren Mitgliedsstaaten der EU, wenngleich die 23 hinzukommenden Fälle einen Rückgang um mehr als 40% gegenüber dem Vormonat darstellen. Die Vorfälle verteilten sich dabei mehrheitlich auf Frankreich mit sechs, Deutschland und Belgien mit vier und Schweden mit drei Vorfällen. Außerhalb Europas wurden zudem vier Vorfälle für die Philippinen aufgenommen, wobei es sich neben einer Earth Karang/I-SOON - die noch in einem ganz anderen Zusammenhang im Februar medial aufgetaucht sind (dazu weiter unten mehr) - zugeschriebenen umfassenden Kampagne um wie eingangs beschriebene hacktivistisch motivierte Vorfälle handelte.

Unter den staatlichen Institutionen, die von Cybervorfällen im März betroffen waren, lassen sich etwa ein Drittel der Vorfälle politisch oder finanziell motivierten DDoS- bzw. Spamming-Angriffen zuordnen, wie gerade etwa für die Philippinen benannt. In Deutschland betraf das etwa die Stadt Fürth mit zwei vermutlich zufällig kurz aufeinander folgenden DDoS-Angriffen im Monat März; in Europa in gleicher Form estnische, luxemburgische und schwedische Behörden. Spamming betraf etwa das Instagram-Profil der italienischen Ministerpräsidentin Giorgia Meloni. In seinen möglichen Schäden weitaus bedeutender war ein Datendiebstahl bei der französischen Arbeitsagentur France Travail, bei dem die Daten von bis 43 Millionen Personen gestohlen wurden. Diese Ereignisse markierten bereits den zweiten Vorfall dieser Art in Frankreich in diesem Jahr, nach den im Februar dieses Jahres bekannt gewordenen Diebstählen bei Almerys und Viamedis. Ebenfalls hohe Wellen schlug ein DDoS-Angriff Mitte des Monats auf Frankreichs interministerielle Behörde für Digitales DINUM, welche etwa die Infrastruktur der französischen Ministerien bereitstellt. Die nachfolgende Debatte und auch internationale Berichterstattung wurde allerdings von Experten angesichts des geringen Schadens als “übertrieben” wahrgenommen. Weiterhin Aufmerksamkeit erzielten bereits berichtete Schwachstellen in Ivanti-Software, die unter anderem bei der für Cybersicherheit zuständigen US-Behörde CISA ausgenutzt wurden, um Zugang zu zwei Systemen zu erhalten.

Geographic distribution of operations



Unter den kritischen Infrastrukturen war - wie im Vormonat - der Finanzsektor mit elf Vorfällen am häufigsten betroffen, gefolgt vom Gesundheitssektor mit neun Vorfällen. Im Finanzsektor lassen sich die Vorfälle etwa hälftig zwei Gruppen zuordnen: Die eine davon betraf sogenannte “Crypto-Heists”, bei denen Hacker unter Ausnutzung von Schwachstellen etwa in Protokollen der Zahlungsdienstleister Geldbeträge abschöpfen können und vermutlich meist unmittelbar finanziell motiviert sind. Die andere Gruppe betraf Datendiebstähle bei (US-amerikanischen) Zahlungsdienstleistern und zugehörigen IT-Dienstleistern. Hier scheint sich die Motivation nicht von Datendiebstählen gegen Unternehmen in anderen Sektoren zu unterscheiden, als es um den möglichen Weiterverkauf der Daten beziehungsweise die Erpressung von Lösegeld geht. Hier ist einschränkend festzustellen, dass für die entsprechenden Vorfälle im März der Einsatz von Ransomware bislang nicht öffentlich dokumentiert ist.

Abweichend zeigt sich die Lage für den Gesundheitssektor, für den in der Mehrzahl der aufgenommenen Vorfälle der Einsatz von Ransomware bestätigt ist oder nahe liegt. Die Konzentration auf diesen Sektor liegt insbesondere in der besonderen Sensibilität der vorhandenen Daten, die ein Druckmittel der meist kriminell operierenden Ransomwaregruppierungen darstellt, weil bei Veröffentlichung für die betroffenen Organisationen möglicherweise neben einem Reputationsverlust auch besonders hohe Schadensersatzzahlungen möglich sind.

Angreiferprofile und Attributionen

Der März weist mit 54% nahezu den gleichen Anteil an vollständig unattribuierten Cybervorfällen wie der Vormonat (53%) auf. Im Vergleich stieg jedoch der Anteil an Operationen, der zwar hinsichtlich des Angreifertyps, nicht aber bezüglich des Ursprungslands näher beschrieben wurde, von 19% auf nun 25%. Die Liste der verzeichneten Ursprungsländer der im März zur EuRepoC-Datenbank hinzugefügten Cybervorfälle hat sich dagegen im Vergleich zum Februar wieder "normalisiert", geht man davon aus, dass die Autokratien wie Russland, China, Nordkorea und Iran, aber auch die Ukraine im Kampf gegen die russischen Angreifer, den beständigen, mittlerweile fest etablierten Kern an besonders aktiven Ländern im Cyberraum ausmachen. Im Vormonat hatte die transnationale Strafverfolgungsoperation "Cronos" zu einer weitaus umfangreicheren und diverseren Liste als in den meisten anderen Monaten geführt und kann daher als eine Abweichung von diesem Muster betrachtet werden. Dennoch erscheint die Ursprungsländer-Liste für den März auch im Vergleich zu vielen anderen Vormonaten stark reduziert, da sich neben den genannten Autokratien mittlerweile auch beständig weitere Länder wie Indien, die Türkei, aber auch Vietnam oder Pakistan Aktivität verzeichneten. Dieser Befund scheint mit der vergleichsweise niedrigeren Fallzahl im März zusammenzuhängen, so war es auch in vereinzelten Vormonaten im Jahr 2023 bereits so, dass bei einer vergleichsweise geringen Fallzahl sich hauptsächlich die vier genannten Autokratien für Operationen verantwortlich zeichneten, die auch ansonsten proaktiv im Cyberraum agieren.

Der Anteil an Cyberoperationen mit attribuierter nichtstaatlicher Verantwortlichkeit (z. B. Hacktivisten, Cyberkriminelle, individuelle Hacker) ist mit 21 Fällen um 5% im Vergleich zum Vormonat gesunken, als dieser Wert noch 35% betrug. Davon zeichneten sich für 11 Operationen kriminelle Akteure verantwortlich, was mit 15% anteilig am Gesamtsample nur etwas weniger sind, als im Februar (17%). Auf Seiten der stärker ideologisch/politisch motivierten Hacktivisten waren es im März nur sechs Fälle, was einen noch deutlicheren Rückgang im Vergleich zum Februar darstellt (von 13% auf 8%).

Der Anteil der sogenannten "Proxy-Operationen", also durchgeführt von staatlich-affiliierten Akteuren, ist dagegen im März von 6% auf 11% angestiegen.

Entsprechend der Fallzahl der Operationen mit nichtstaatlicher Verantwortlichkeit ist auch die Selbstattribution (21 Mal) als häufigste Attributionsquelle im März vertreten. Dahinter rangieren Threat Intelligence Unternehmen, im März wurden acht technische Berichte, die Attributionen enthielten, in den Datensatz aufgenommen. In fünf Fällen stammte die Verantwortungszuweisung dagegen von politischen/staatlichen Akteuren des betroffenen Landes. Solche politische Attributionen erfolgen zumeist recht wenig formalisiert, etwa über Statements in Medienberichten, oder über kurze Presseerklärungen auf den Ministerialwebseiten. Eine dieser fünf Attributionen fand jedoch im Rahmen einer strafrechtlichen Maßnahme des US Department of Justice statt. In seiner Anklageerhebung vom 29. Februar 2024 veröffentlichte das Ministerium den Namen eines Mitarbeiters einer iranischen Tarnfirma, Mahak Rayan Afraz (MRA), die

laut der Anklage im Auftrag der iranischen Revolutionsgarden Hacking-Operationen durchführt. So wurde dem Angeklagten Alireza Shafie Nasab vorgeworfen, an der Kompromittierung von US-Netzwerken von Regierungsorganisationen und privaten Unternehmen (u.a. Rüstungskonzernen) zwischen 2016 und April 2021 beteiligt gewesen zu sein. Bereits am 16. Februar dieses Jahres hatte das US State Department im Rahmen des “Rewards for Justice” Programms 10 Millionen Dollar Belohnung für bedeutende Informationen über Nasab ausgelobt. Diese sequenziert erfolgenden, in Teilen auch aufeinander aufbauenden Maßnahmen unterschiedlicher staatlicher Behörden, gerichtet gegen ein und dieselbe Person, jedoch mit unterschiedlichen Zielsetzungen und Wirkmechanismen, verdeutlichen den immer stärker angewandten “Whole-of-government”-Ansatz der USA im Cybersicherheitsbereich. Dabei setzen die USA nicht nur im Rahmen gemeinsamer Attributionserklärungen verstärkt auf die Zusammenarbeit unterschiedlicher US-Behörden und Ministerien, sondern auch für die Vorbereitung, Koordinierung und Durchführung nachgelagert oder im Verbund erfolgender Strafverfolgungsoperationen.

Die Anklage gegen Nasab wurde am 23. April um weitere Angeklagte erweitert, nämlich die ebenfalls aus dem Iran stammenden Hossein Harooni, Reza Kazemifar und Komeil Baradaran Salmani, die für die gleichen Hackingoperationen wie Nasab angeklagt wurden. Warum die Anklagen im Zweimonatsabstand veröffentlicht wurden und nicht zusammen im Februar oder im April erhoben wurden, kann nicht beurteilt werden. Vorstellbare wäre aber, dass es in der Zwischenzeit noch wichtige Erkenntnisgewinne gab, die letztlich auch die Anklage der weiteren Personen ermöglichte, oder aber andere verfahrenstechnische oder taktische Gründe für dieses Vorgehen maßgeblich waren, zumal sie im selben New Yorker District und vom selben Staatsanwalt erhoben wurden.

Der Fall verdeutlicht darüber hinaus einmal mehr das bestehende System aus iranischen Unternehmen, die um staatliche Hackingaufträge konkurrieren und in dieser Rolle immer häufiger in das Fadenkreuz vor allem US-amerikanischer Ermittler:innen geraten. Ähnlichkeiten weist dieses Proxy-Modell mit chinesischen Vertragsnehmern der Volksbefreiungsarmee, sowie vor allem des Ministeriums für Staatssicherheit (MSS) auf, die ebenfalls in großem Umfang

einheimische Unternehmen mit aufbauen und dann in einem immer härter werdenden Wettstreit um staatliche Aufträge treten lassen. Besondere Aufmerksamkeit erfahren hat dabei ein umfangreiches Leak der chinesischen Firma I-SOON von Ende Februar. Hierbei war ein erhebliches Ausmaß der Aktivitäten nur dieses einen Vertragsnehmers chinesischer Behörden im Hacking- und Überwachungsbereich öffentlich geworden. Gleichzeitig hat es jedoch auch die Probleme solcher Unternehmen verdeutlicht, an genügend Aufträge zum eigenen Überleben zu gelangen, was zu umfangreichen Werbemaßnahmen der Hacking- und Überwachungsfähigkeiten gegenüber potentiellen Auftraggebern führte. Dies wirft für die Zukunft auch die Frage auf, inwiefern sich solche Akteure als Konsequenz dann auch immer häufiger auf finanziell motivierte Ransomware-Operationen verlagern, um die entgangenen Gewinne aus nicht erhaltenen staatlichen Aufträgen besser kompensieren zu können. I-SOON hatte besonders auch dem chinesischen Ministerium für öffentliche Sicherheit (MPS) zugearbeitet, das vor allem für Überwachung im Inneren verantwortlich ist, gegenüber den noch stärker nach außen gerichteten Hackingoperationen des MSS.

Die Zahl an Cyberoperationen im Kontext des russischen Krieges gegen die Ukraine ist trotz der insgesamt im Vergleich zum Februar gesunkenen Fallzahl um zwei Vorfälle gestiegen. Von den sieben Fällen wurden sechs (pro-)russischen Akteuren zugesprochen, bzw. von diesen selbst für sich reklamiert. Nur ein Fall von Cyberspionage, richtete sich vom ukrainischen Geheimdienst gegen das russische Verteidigungsministerium.

Mehr von EuRepoC

Seit April können Interessierte als neues Angebot EuRepoC's "Critical Infrastructure Tracker" verwenden. Der Tracker liefert interaktive Analysetools zu unterschiedlichen Aspekten von Cyberoperationen, die kritische Infrastrukturen in Deutschland, Europa und Drittländern betroffen haben, etwa die anvisierten Teilsektoren, die attribuierten Angreifer, sowie die Verbindungen zu bestehenden konventionellen Konflikten.

EuRepoC-Forscher Jakob Bund präsentierte gemeinsam mit Microsoft den möglichen Einsatz von Copilot zur erweiterten Analyse der Cyberkonfliktdaten von EuRepoC am 23. April auf der diesjährigen European Cyber Agora in Brüssel.

EuRepoC informiert 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 Wissenschaftlerin 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).