European
Repository of
Cyber Incidents

EuRepoC

Cyber Conflict Briefing

Juni 2024

Jakob Bund
Kerstin Zettl-Schabath
Martin Müller

Beobachtungen zur Gesamtlage

Im **Juni 2024** wurden 60 Cyber-Operationen in die EuRepoC-Datenbank aufgenommen. Das sind 17,8% weniger als im Vormonat und 11 Operationen weniger als die insgesamt durchschnittlich verzeichnete Aktivität von 71 Cyber-Operationen pro Monat im Gesamtzeitraum.

Die **durchschnittliche Intensität** der im Juni 2024 erfassten Operationen beträgt 3,15 und liegt somit über dem historischen Durchschnitt (2,84). 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 Juni stattgefunden haben, sondern können bereits zu einem früheren Zeitpunkt begonnen haben. Dabei stehen technische, politische sowie rechtliche Aspekte im Vordergrund.

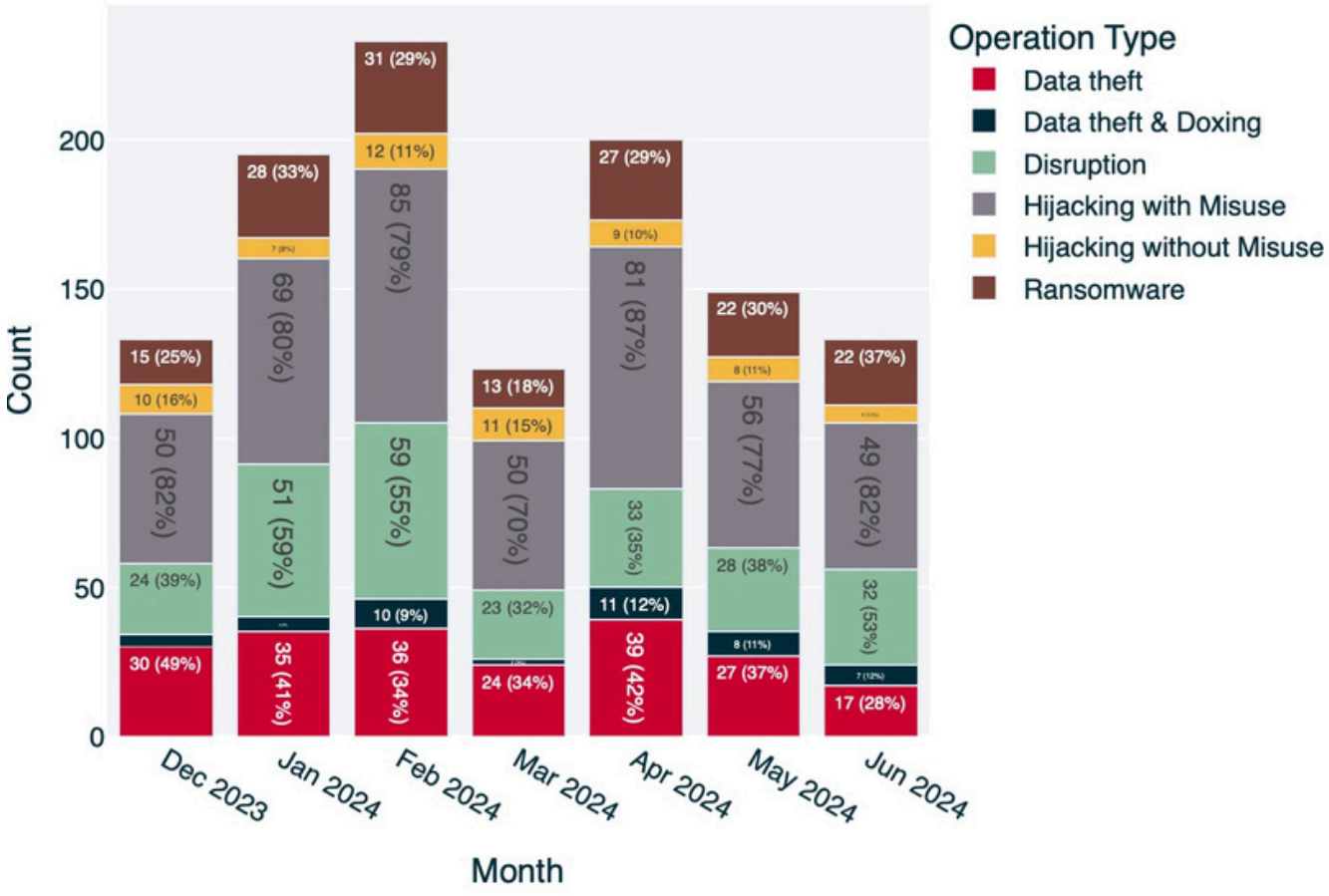
Über EuRepoC

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

Monthly distribution of operations



Hinweis: Einzelne Cybervorfälle können mehrere Operationstypen in Kombination aufweisen.

Der zweithäufigste im Juni 2024 festgestellte Operationstyp war 'Disruption'-Operationen (53%). 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. Im Fall von Ransomware kann der blockierte Zugriff auf betriebswichtige Daten allerdings auch über einen längeren Zeitraum für Ausfälle sorgen. Von diesen Operationstypen sind für Juni 32 durch das Repositorium erfasst.

Den größten Anteil umfassten jedoch 'Hijacking with Misuse' - Operationen mit 49 Fällen (82%). 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 Motive hinter diesen Aktivitäten können sich auch überschneiden und im zeitlichen Verlauf ändern. Entsprechende Spekulationen kamen Anfang Juni auf, nachdem die Ransomwaregruppe BianLian umfangreiche Daten des australischen Bergbauunternehmens Northern Minerals veröffentlichtet hatte. Von dem Leak betroffen waren Details zu betrieblichen Prozessen, Projektdokumente, Forschungs- und Entwicklungsdaten, finanzielle Informationen, sowie Daten von Mitarbeitenden und Investoren. Am selben Tag hatte der australische Finanzminister Jim Chalmers mit Verweis auf nationale Interessen fünf Firmen mit Verbindungen nach China angewiesen, sich aus ihrem Investment in Northern Minerals zurückzuziehen. Diese zeitliche Nähe weckte in Medienberichten unbestätigte Vermutungen, BianLian könnte Interna des Förderunternehmens in Vergeltung für diese Anordnung geleakt haben, entweder auf direktes Geheiß offizieller Stellen in China oder auf eigene Initiative, um sich staatliches Wohlwollen zu sichern.

Northern Minerals Fördertätigkeit in Australien ist unter anderem mit der Erschließung strategisch wichtiger Lagerstätten von Seltenen Erden befasst. In der Vergangenheit haben sich chinesische Vergeltungsmaßnahmen in Antwort auf vermeintlich unfaire Investitions- und Handelsbeschränkungen wiederholt auf Chinas Kontrolle über die natürlichen Vorkommen und industriellen Prozesse zur Gewinnung dieser Rohstoffe konzentriert. Im Juli 2023 etwa reagierte Chinas Handelsministerium auf gemeinsame Exportkontrollen für Halbleiterherstellungsausrüstung der USA, Japans und der Niederlande mit Ausfuhrbeschränkungen für Seltene Erden, die für die Fertigung von Computerchips benötigt werden. Später in 2023 weitete die chinesische Regierung ein bestehendes Exportverbot auf zusätzliche für die Verarbeitung von Seltenen Erden verwendete Technologien aus.

BianLians Einbruch in die eigenen Netzwerke hatte Northern Minerals bereits Ende März entdeckt. Die Firma nahm allerdings erst am Tag nach der Veröffentlichung der gestohlenen Daten, am 4. Juni, öffentlich Stellung zu den Vorkommnissen.

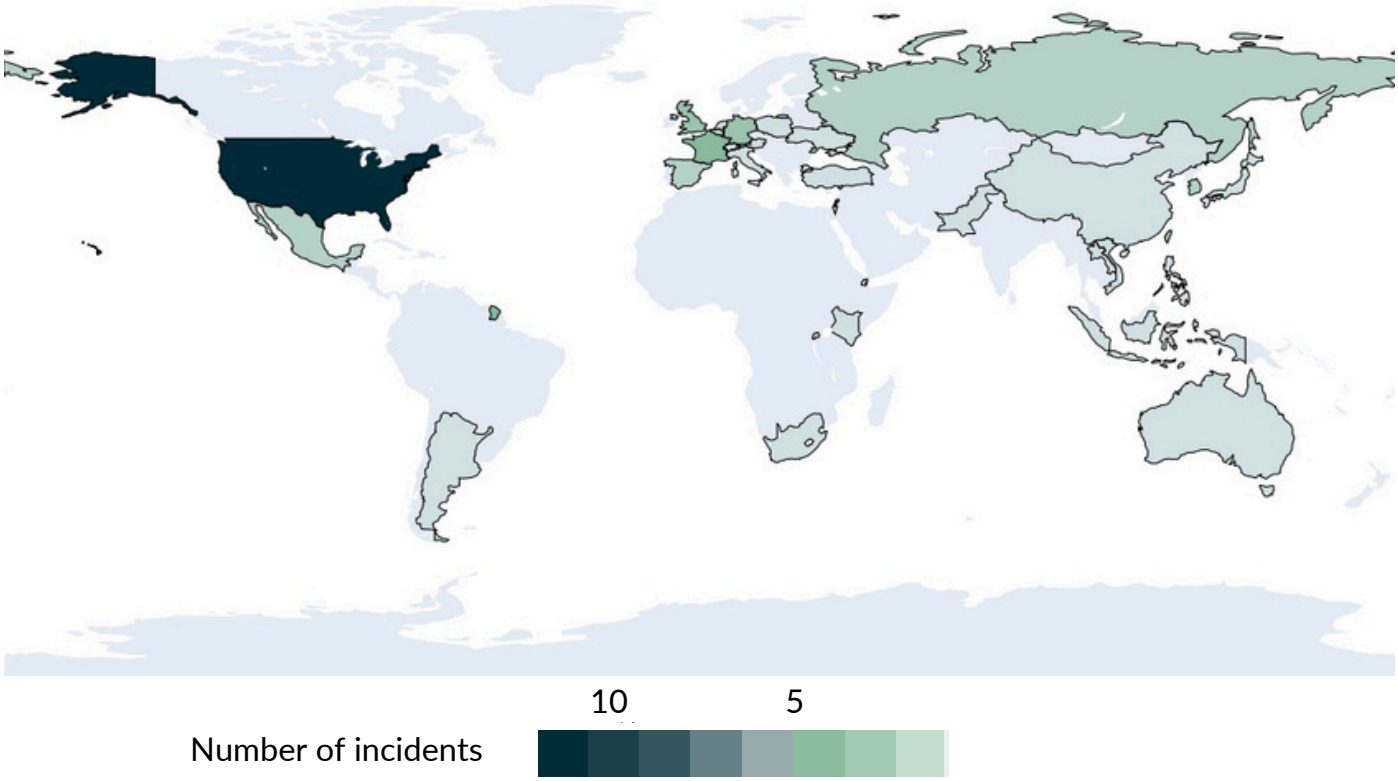
Dass BianLian erbeutete Opferdaten erst mit mehreren Wochen Abstand preisgibt, ist grundsätzlich nicht ungewöhnlich für die Gruppe. Verzögerungen sind insbesondere zu erwarten, wenn anfängliche Gespräche mit betroffenen Unternehmen im weiteren Verlauf scheitern.

Australiens Schattenminister für innere Angelegenheiten James Patterson forderte eine deutliche Reaktion der Regierung, sollte sich herausstellen, dass BianLians Aktionen auf staatliche Unterstützung zurückgehen. Für eine derartige Vermischung von finanziellen und geopolitischen Motiven bestehen aktuell keine belastbaren Hinweise. Nach bisherigen Erkenntnissen kann sich der zeitliche Zusammenhang zwischen BianLians Leak von Northern Minerals-Daten und dem durch die australische Regierung angeordneten Verkauf von Firmenanteilen auch zufällig ergeben haben.

Brennpunkte und Zielmuster

Der am häufigsten im Juni betroffene Zielsektor waren - wie in den Vormonaten schon beobachtet - Unternehmen der kritischen Infrastruktur. In diesem Monat waren dies 36 Fälle, was bezogen auf die Gesamtzahl von neu aufgenommenen 60 Fällen drei von fünf aller Fälle entspricht. Am zweithäufigsten waren in 25 Fällen beziehungsweise 42% staatliche

Geographic distribution of operations



Institutionen betroffen. Mit dem Rückgang an neu aufgenommenen Vorfällen gegenüber dem Mai ist damit die Zahl der kritische Infrastruktur betreffenden Vorfälle insgesamt um 20% gesunken. Dies macht sich bei den staatlichen Institutionen geringer bemerkbar, weil hier nur ein Fall weniger als im Vormonat Mai aufgenommen wurde.

Am häufigsten betroffen waren erneut die Vereinigten Staaten mit zwölf Vorfällen. Etwas häufiger betroffen waren in 16 Vorfällen Mitgliedsstaaten der EU, wobei hier Frankreich mit fünf und Deutschland mit drei Fällen die meisten Vorfälle verzeichneten. Drei Vorfälle wurden in der EuRepoC-Datenbank auch für Großbritannien und Taiwan verzeichnet.

Unter den Unternehmen der kritischen Infrastruktur wurden mit acht Fällen die meisten im Bereich der Finanzunternehmen verzeichnet. Hier war eine paritätische Verteilung zwischen Dienstleistern im Kryptowährungssektor und jenem „klassischer“ Finanzunternehmen zu verzeichnen. Wie in den Vormonaten schon beobachtet, werden für den Kryptosektor fast ausschließlich sogenannte „Crypto Heists“ verzeichnet, welche unmittelbar finanzielle Motive verfolgen und hierfür Schwachstellen in den Protokollen dieser Dienstleister ausnutzen. Für klassische Finanzunternehmen hingegen wurden wie im Fall einer DZ Bank-Tochter in Deutschland im Juni ausnahmslos Datendiebstähle kodiert, die hier unter Umständen im Einsatz mit Ransomware eher dazu dienen, die Unternehmen aus Angst vor Rufschädigungen oder aufsichtsrechtlichen Sanktionen zu Verhandlungen zu bewegen. Ein anderes Motiv liegt auch darin, durch die erlangten Daten zielgerichtetere Angriffsmethoden, etwa im Bereich des Phishing, zu unterstützen.

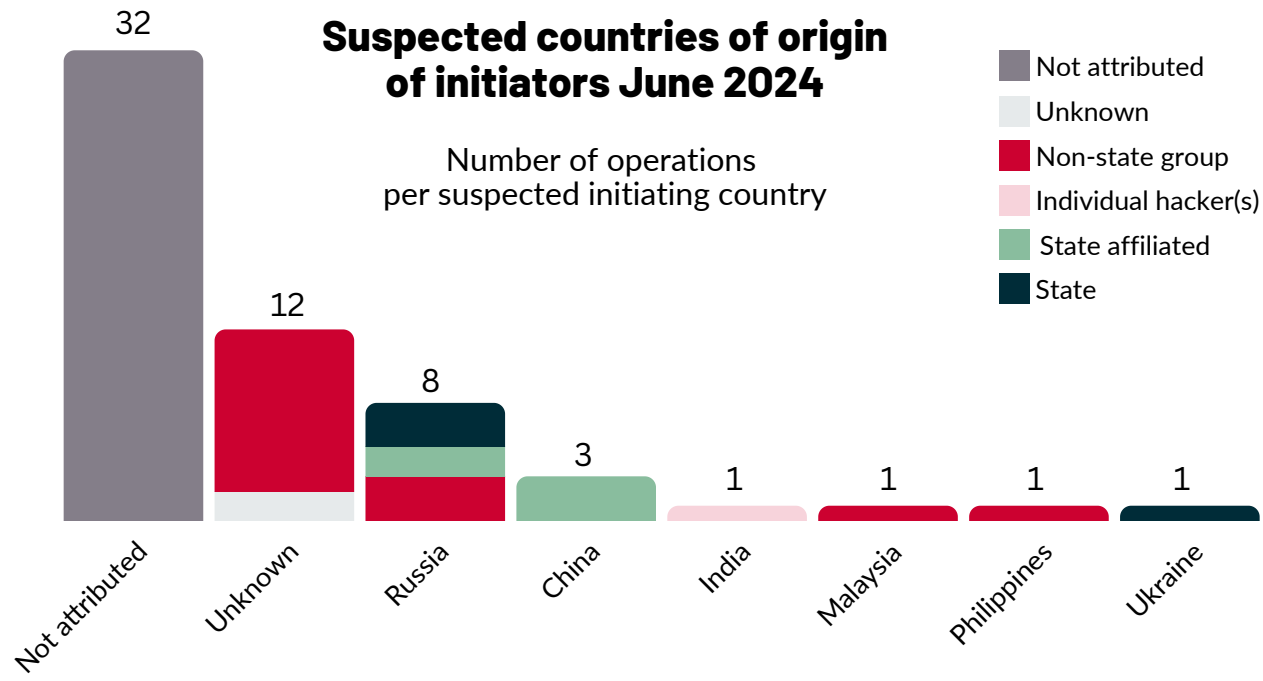
Weiterhin häufig betroffen war der Gesundheitssektor als kritische Infrastruktur, im Juni in sieben Fällen. Anders als für die vergangenen Monate beobachtet, konzentrierten sich diese geographisch nicht auf US-amerikanische

Einrichtungen, sondern auf europäische. Schlagzeilen machte etwa ein Ransomwareeinsatz gegen Synnovis, einem Dienstleister des britischen NHS, der unter anderem die Verschiebung wichtiger Operationen im Raum London zur Folge hatte.
Unter den staatlichen Institutionen war erneut eine deutliche Mehrzahl an sub-nationalen, behördlichen Einrichtungen betroffen; im Juni waren dies 16 Vorfälle, gefolgt von Einrichtungen auf nationaler Ebene in fünf Vorfällen. Hier wurde in überhaupt nur zwei Fällen Ziele bekannt, wobei beide Fälle Frankreich betrafen. Zunächst wurden Mitte des Monats eine Vielzahl von Regierungswebsites durch DDoS-Angriffe gestört und waren kurzfristig nicht erreichbar. Weiterhin wurde durch ANSSI, der französischen Cybersicherheitsehörde, eine seit 2021 laufende Spionagekampagne gegen diplomatische Einrichtungen offengelegt.
Auf sub-nationaler Ebene bleibt die Gefahrenlage im Cyberraum dagegen diffus: Neben dem durchweg zu beobachteten Einsatz von Ransomware, sind beispielsweise in Belgien auch politisch motivierte Vorfälle wie DDoS-Angriffe oder Defacements zu beobachten.

Angreiferprofile und Attributionen

Der Juni weist mit 53 % einen um 5 % gesunkenen Anteil an komplett unattribuierten Cybervorfällen im Vergleich zum Vormonat Mai (58 %) auf. Der Anteil an Operationen, der zwar hinsichtlich des Angreifertyps, nicht aber bezüglich des Ursprungslands näher benannt wurde, stieg von 15 % im Mai auf nun 22 %.

Die Liste der verzeichneten Ursprungsländer der im Juni zur EuRepoC-Datenbank hinzugefügten Cybervorfälle umfasst im Vergleich zu den meisten Vormonaten diesmal weder Iran noch Nordkorea. Stattdessen finden sich darin diesmal Malaysia, die Philippinen sowie Indien mit jeweils einem Fall wieder. In allen drei Fällen wurden nichtstaatliche Akteure, mit teilweise kriminellen oder eher ideologischen, bzw. sogar persönlichen Motiven verantwortlich gemacht. So hat die Cyberkriminellen-Gruppierung DragonForce das öffentliche Transportunternehmen Oahu Transit Services auf Hawaii mit Ransomware getroffen. Hinsichtlich der in Medienberichten getätigten Attribution Malaysias als Ursprung der Gruppierung ergeben sich jedoch gewisse Zweifel: so ist nicht klar ersichtlich, ob nicht lediglich die für die noch besser bekannte Hacktivisten-Gruppierung DragonForce Malaysia bestehende Länderzuweisung einfach übernommen wurde. Während sich die im vorliegenden Fall verantwortliche Gruppierung auf finanziell motivierte Ransomware konzentriert, tätigt DragonForce Malaysia insbesondere DDoS und Defacement-Operationen gegen indische Ziele, hat sich aber auch im Rahmen von Aktivitäten gegen israelische Ziele auch als pro-palästinensisch gezeigt. Die Gruppe hat die durch Threat-Intelligence-Analysten mehrfach hergestellte Verbindung zur Ransomware-Gruppe mit dem gleichen Namen zudem bereits geleugnet. Mit als Erstes auf Social Media darüber berichtet hat das indische Threat Intelligence Unternehmen FalconFeeds, für deren Kunden potenziell beide Gruppen, vor allem aber DragonForce Malaysia, von Relevanz sein dürfte. Jedoch auch für Ransomware-Gruppierungen spielen aufgrund der Bedeutung der Täter-Opfer-Kommunikation, etwa im Rahmen von Lösegeldverhandlungen, potenzielle Sprach- und Kulturbarrieren eine wichtige Rolle, weshalb oft auch regionale Zielmuster festzustellen sind. Eine Ausnahme hiervon sind Gruppierungen wie etwa russische, deren „Abmachung“ mit den jeweiligen



Heimatland-Behörden gerade vorsehen, diesen Raum von ihren Aktivitäten auszuschließen, um weiterhin weitestgehend unbehelligt agieren zu können. Der breit angelegte Einsatz generativer KI-Chatbots wie ChatGPT und deren Integration in Angriffsstrukturen könnte dieses Regionalmuster jedoch in Zukunft auch für andere Gruppierungen, z.B. aus Asien, zumindest graduell verändern.

Auch der Fall mit indischer Täterschaft ist von Interesse, verdeutlicht er einmal mehr die oft unterschätzte Gefahr von Insidern, gerade, wenn diese gegen ihren Willen aufgrund von Entlassungen kürzlich zu Outsidern geworden sind: Der indische Staatsangehörige Kandula Nagaraju verschaffte sich Zugang zu einer Testumgebung des in Singapur ansässigen Informationstechnologieunternehmens National Computer Systems (NCS) und löschte vom 6. Januar bis zum 19. März 2023 dessen 180 virtuelle Server, berichteten Medien unter Berufung auf Nagarajus entsprechende Verurteilung am 10. Juni 2024. Kandula Nagaraju, 39, war in der Abteilung für Qualitätssicherung (QA) von NCS beschäftigt, bis sein Arbeitsvertrag im Oktober 2022 gekündigt wurde. Aus Rache begann er ab dem 6. Januar 2023, mit seinen früheren Zugangsdaten auf das NCS-Netzwerk zuzugreifen. Dies tat er bis zum 17. Januar 2023, dann erneut am 23. Februar 2023, bis er vom 18. bis 19. März 2023 die 180 virtuellen Server in einer Testumgebung der Qualitätssicherungsabteilung löschte und damit einen Schaden von 918.000 USD verursachte. Das Gericht befand ihn des unbefugten Zugriffs auf Computermaterial für schuldig und verurteilte ihn zu einer Haftstrafe von zwei Jahren und acht Monaten.

Auf Seiten der prävalenten konventionellen Konflikte dominierte auch im Juni einmal mehr der Krieg zwischen Russland und der Ukraine, mit sechs verzeichneten Vorfällen. Des Weiteren wurden drei Konfliktdyaden mit jeweils einer zugeordneten Cyberoperation aufgenommen, nämlich China (Taiwan), Israel (Hamas et al.) und Vietnam et al. – China im Kontext der Streitigkeiten um das Südchinesische Meer.

Es ist seit langem bekannt, dass russische Geheimdienste enge Verbindungen zu Cyberkriminellen im post-sowjetischen Raum unterhalten und bei deren Tätigkeiten zum einen „wegschauen“, insofern nicht russische Ziele anvisiert werden und sich die Hacker von Zeit zu Zeit auch als staatliche

Stellvertreter, sog. „Cyber-Proxies“ betätigen. Dass dabei oftmals unterschiedliche Motivlagen auf Seiten der zivilen Hacker dazu führen, dass sie sich irgendwann sogar auf den Fahndungslisten des FBI, sowie als Angeklagte des US Department of Justice wiederfinden können, zeigt potenziell die Anklageschrift gegen Amin Stigal, die am 26. Juni veröffentlicht wurde: Darin werfen die US-Behörden dem in der tschetschenischen Hauptstadt Grosny geborenen, heute 22-Jährigen vor, gemeinsame Sache mit dem militärischen Geheimdienst GRU gemacht zu haben. So habe er diesem zwischen August 2021 und Februar 2022 dabei geholfen, ukrainische Ziele zu hacken, die Rede ist etwa von der bekannten Wiper-Attacke „WhisperGate“ im direkten zeitlichen Vorfeld der russischen Invasion Ende Februar 2022. Nicht nur ukrainische, sondern auch amerikanische Ziele aus dem Regierungs- sowie Privatsektor finden sich ebenfalls unter den berichteten Opfern Stigals und des GRU. In der Anklageschrift sind keine weiteren Details zur „Anbahnung“ der Zusammenarbeit zwischen Stigal und dem GRU enthalten, sodass sich lediglich Mutmaßungen über dessen Motivation anstellen lassen. Zwei Dinge bieten hierfür Anhaltspunkte: Erstens, ist Stigal wie viele andere Hacker noch sehr jung und startete seine Karriere als russischer „hacker-for-hire“ bereits mit 19 Jahren. Wie wichtig es wäre, neben Abschreckung durch Bestrafung bei der Prävention von Cyberkriminalität bereits im Jugendalter auf Sozialisationsmaßnahmen zu setzen, betont das „Cyber Offender Prevention“-Programm der niederländischen Sicherheitsbehörden, die umfassende Kampagnen für technisch begabte Jugendliche entwickelt haben, um diesen die Illegalität von Cyberkriminalität einerseits, aber auch die bestehenden Möglichkeiten zur legalen Anwendung ihrer Fähigkeiten andererseits zu demonstrieren. Gerade in Ländern, in denen Jugendliche nur wenige Möglichkeiten auf dem Arbeitsmarkt haben, was sowohl in Tschetschenien, als auch in der Republik Dagestan, zu der Stigal laut FBI-Profil ebenfalls Beziehungen unterhalten soll, der Fall ist, besteht die Gefahr, dass sie sich der drittgrößten Volkswirtschaft der Welt zu wenden, der Cyberkriminalität. Stigals Verbindungen zu Dagestan könnten zumindest partiell auch eine ideologische Motivlage für die Hacking-Operationen in den Diensten des Kremls bedeuten, zeigten sich doch Teile der Bevölkerung Dagestans in der jüngeren Vergangenheit besonders Putin-begeistert. Ökonomische Perspektivlosigkeit, gepaart mit ideologischer Überzeugung, stellt für nichtstaatliche Hacker eine Kombination dar, die sie besonders attraktiv für autokratische Regime und deren Sicherheitsbehörden werden lässt, beides könnte im Falle Stigals von Anfang an vorgelegen, oder sich im Laufe der Zeit herausgebildet haben.

Dass auch die VR China weiterhin ihre geopolitischen Ziele, besonders in Asien und Afrika, auch im Cyberraum verfolgt, wurde auch im Juni deutlich. Von November 2023 bis April 2024 führte die staatlich finanzierte chinesische APT RedJuliett, bei Microsoft auch als Flax Typhoon bekannt, eine Spionagekampagne durch, die hauptsächlich auf Taiwan abzielte, aber auch Einrichtungen in Hongkong, Kenia, Südkorea, Ruanda, Dschibuti, Laos und den USA betraf. Bei dieser Operation wurden insgesamt 24 Organisationen in Bereichen wie dem Regierungssektor, Technologie, Wissenschaft und auf der Ebene der diplomatischen Beziehungen kompromittiert. Im Gegensatz zur chinesischen Gruppierung Volt Typhoon, deren Infiltrationen amerikanischer kritischer Infrastrukturen letztes Jahr nicht nur als Cyberspionage, sondern als Vorbereitungshandlungen potenzieller Sabotageakte von Microsoft gewertet

wurden, bleibt eine ähnliche Unterstellung für Flax Typhoon bislang noch aus, die Kampagne öffentlich gemacht hat das Threat Intelligence Unternehmen Recorded Future. EuRepoC wird in Kürze ein vergleichendes APT-Profil für Volt Typhoon und Flax Typhoon veröffentlichen, das Gemeinsamkeiten und Unterschiede beider Gruppen genauer beleuchtet.

Mehr von EuRepoC

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.