European
Repository of
Cyber Incidents

EuRepoC

Cyber Conflict Briefing

November 2023

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

Beobachtungen zur Gesamtlage

Im **November 2023** wurden 76 Cyber-Operationen in die EuRepoC-Datenbank aufgenommen. Das sind 4% weniger als im Vormonat, aber 17 Operationen mehr als die insgesamt durchschnittlich verzeichnete Aktivität von 58 Cyber-Operationen pro Monat im Gesamtzeitraum.

Die **durchschnittliche Intensität** der im November 2023 erfassten Operationen beträgt 3,13 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 November stattgefunden haben, sondern können bereits zu einem früheren Zeitpunkt begonnen haben. Dabei stehen technische, politische sowie rechtliche Aspekte im Vordergrund.

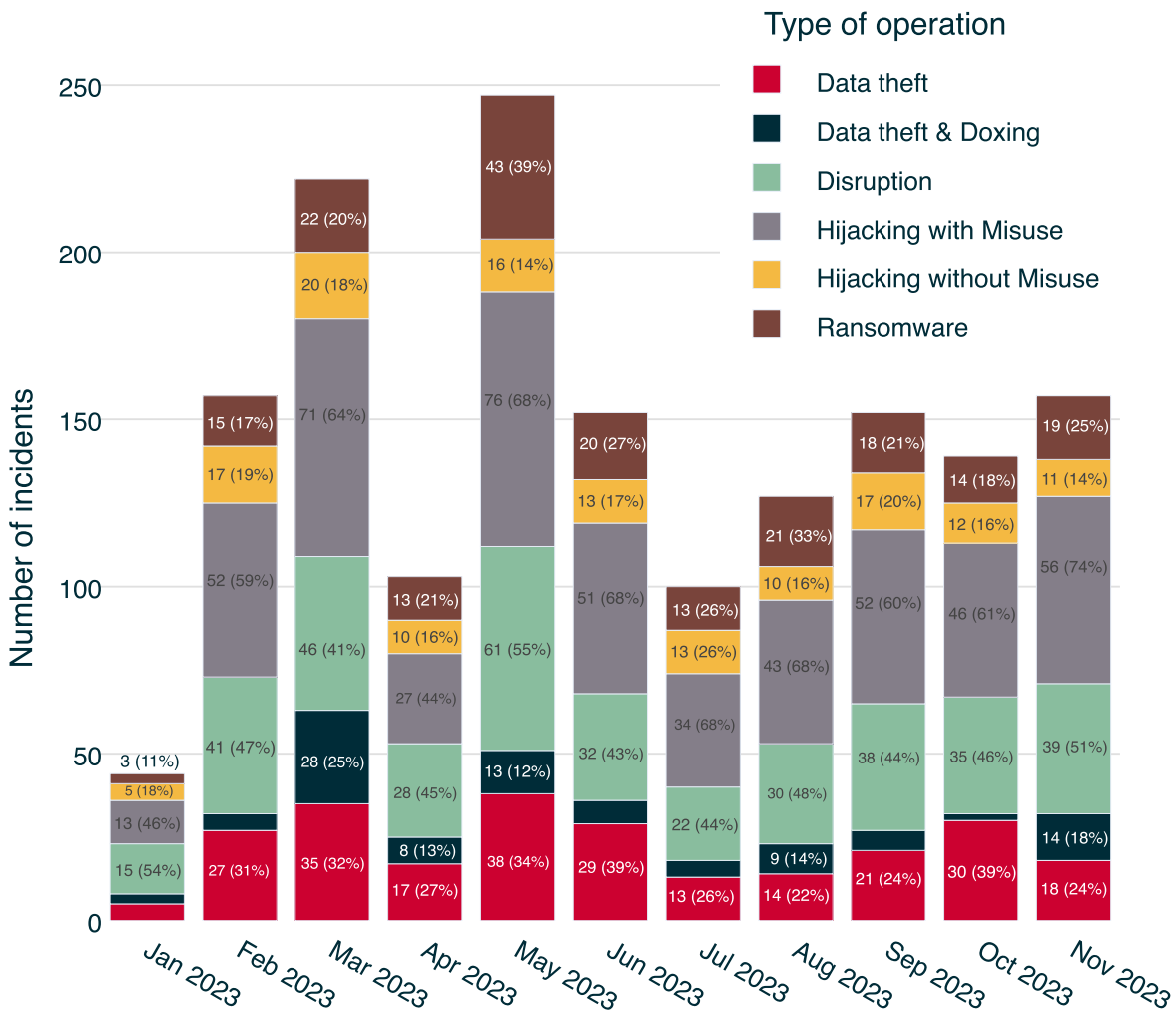
Über EuRepoC

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 November 2023 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 56 Fällen (74%). 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.

Wie letzten Monat im Zusammenhang mit StripedFly, einer als Cryptominer getarnten Spionageoperation beschrieben, stellt die Bewertung von Motiven gerade in Hinblick auf „Hijacking with Misuse-Operation" auch für über Jahre beobachtete Aktivitäten eine anhaltende Herausforderung dar. Diese Schwierigkeiten bestehen auch dann, wenn zwar ein Abfluss von Daten zu erkennen ist, die Verwendung der gestohlenen Informationen aber nicht direkt nachvollziehbar ist.

In einem Präzedenzfall hat der ukrainische Militärgeheimdienst GUR Ende November nicht nur eine eigene offensive Cyberoperation offenlegt und erlangte Daten veröffentlicht, sondern diese im Rahmen einer Presseerklärung genutzt, um die Bedeutung internationaler Sanktionen gegen Russland zu unterstreichen und direkt in eigene strategische Narrative einzubinden.

Konkret ist es dem GUR nach diesen Schilderungen gelungen, in Netzwerke einzudringen, über die der Dienst Zugriff auf vertrauliche Berichte von Russlands ziviler Luftfahrtbehörde Rosaviatsia erlangte.
Die Berichte, die sich über einen Zeitraum von mehr als anderthalb Jahren erstrecken und sicherheitsrelevante Zwischenfälle und Fehlfunktionen dokumentieren, lassen auf erhebliche Schwierigkeiten in der Befolgung von Wartungsanforderungen schließen.
Nach diesen Meldungen sind knapp 70% der Flugzeuge aus russischen Flotten nur durch Prüfungen in nicht zertifizierten Wartungsbetrieben und den Einsatz von nachgebauten Ersatzteilen in Funktion zu halten.

In der offiziellen Mitteilung über die Operation listet der GUR mutmaßlich aus den Dokumenten gewonnene Erkenntnisse über den Zustand der russischen Luftfahrtsicherheit im Detail und verweist auf den geleakten Datensatz.
Vor dem Hintergrund dieser Auswertung kommuniziert die Presseerklärung außerdem die Einschätzung, dass internationale Sanktionen maßgeblich zu dieser Situation beigetragen haben und hebt dabei Verbote von Lieferungen von Flugzeugen und Ersatzteilen; die Verweigerung von Software-Updates; die Beschlagnahme von russischen Flugzeugen im Ausland; und die Beschränkung des Zugangs zu meteorologischen Informationen für die Flugnavigation hervor.

Ausführungen des ukrainischen Verteidigungsministeriums zeichnen die Auswirkungen von Sanktionen mitverantwortlich für die Entscheidung der Internationalen Zivilluftfahrtorganisation (ICAO) im September 2022, Russland erhebliche Sicherheitsbedenken auszusprechen und Russland als nur eines von fünf Ländern mit diesem Status zu belegen. Die ICAO war im Februar 2022 auch die erste UN-Organisation, die den Einmarsch Russlands in die Ukraine verurteilte.

Der zweithäufigste im November festgestellte Operationstyp war „Disruption“-Operationen (51%). 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 November 39 durch das Repositorium erfasst.

Im Rahmen von geopolitischen Spannungen sind in seltenen Fällen auch Sabotageversuche unter Disruption-Operationen beobachtet. Der russische Bedrohungsakteur Sandworm etwa verschaffte sich im Juni 2022 Zugang zu den operativen Steuerungssystemen eines ukrainischen Stromversorgers und zerstörte im darauffolgenden Oktober Daten mit einer abgewandelten Variante des CADDYWIPER, wie das Threat-Intelligence-Unternehmen Mandiant am 9. November 2023 berichtete. CADDYWIPER war zuerst durch die Cybersicherheitsfirma ESET kurz nach dem russischen Großeinmarsch Mitte März 2022 in Angriffen gegen ukrainische Ziele beobachtet worden.

Sandworm verschaffte sich Zugang zur Zielumgebung über einen Hypervisor, eine Software, die eine unabhängige Computerumgebung simuliert. Über diesen Zugriff gelang es Sandworm, angeschlossene industrielle Steueranlagen, sogenannte SCADA-Systeme, zu erreichen, über die das betroffene Energieunternehmen Umspannwerke überwacht. Am 10. Oktober 2022 löste die russische Gruppe die darüber kontrollierten Leistungsschutzschalter eines Umspannwerks aus und verursachte einen Stromausfall.

Im Unterschied zu vorausgehenden Versuchen, die ukrainische Stromversorgung zu kappen, zeichnen sich Sandworms zuletzt berichtete Aktionen durch Bestrebungen aus, dieses Ziel möglichst unter Verwendung von systemeigenen Werkzeugen zu erreichen – eine Taktik, die allgemein als „living off the land“ beschrieben wird.

Diese Techniken ermöglichen die Tarnung des eigenen Vorgehens als vermeintlich normales Betriebsverhalten. Neben der Bemühung, dadurch einer Entdeckung zu entgehen, könnten dabei auch Überlegungen, damit das eigene Arsenal zu schonen und eine Abnutzung der eigenen Fähigkeiten zu verhindern, eine Rolle gespielt haben – Erwägungen, die in Anbetracht von Entwicklungen eines Zermürbungskriegs an Gewicht gewinnen.

Zwei Tage nach der erzielten Stromunterbrechung verursachte Sandworm allerdings eine weitere Störung, durch den Einsatz des erwähnten CADDYWIPER in den IT-Netzwerken des Stromanbieters. Da der Wirkungsbereich des Wipers auf die IT-Umgebung beschränkt war, hatte diese Aktion keine unmittelbare Auswirkung auf für die Aufrechterhaltung der Stromversorgung zuständigen Systeme.

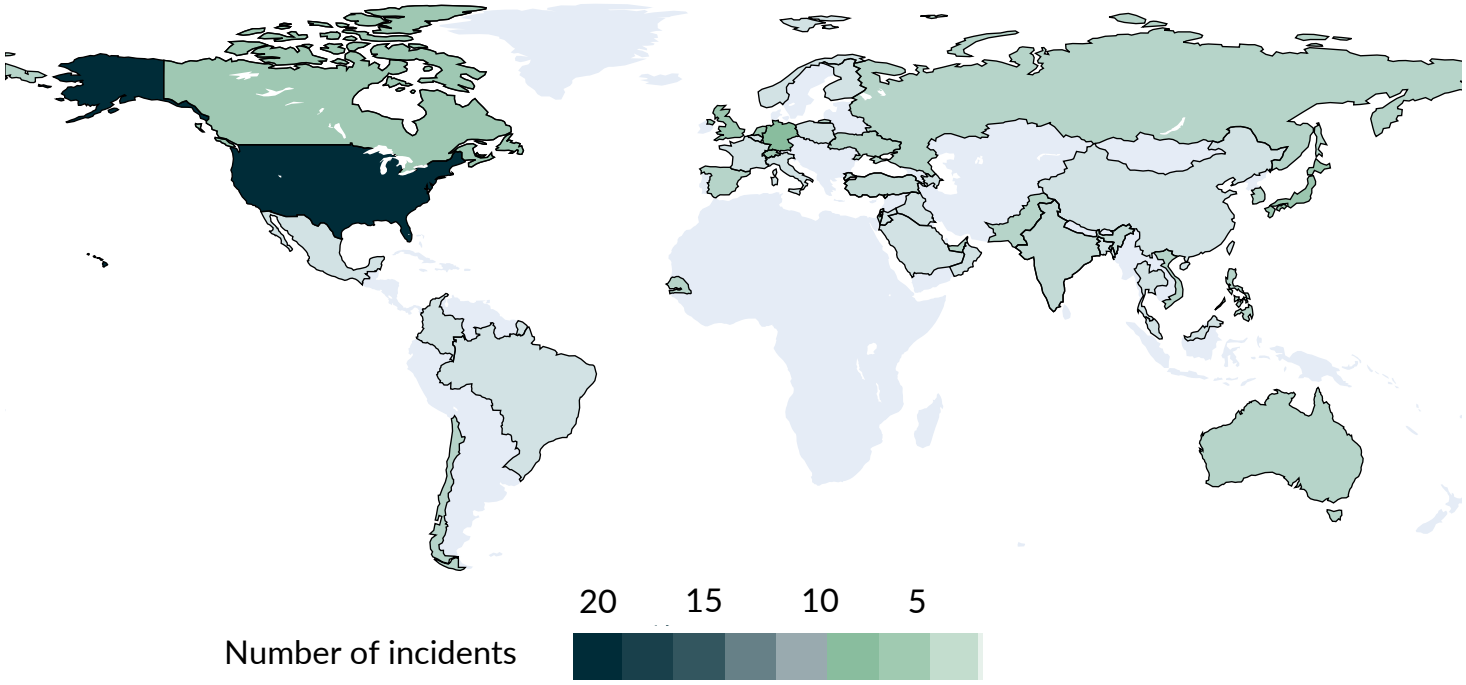
In letzteren hatte Sandworm eigentlich zuvor versucht, die Spuren der eigenen Aktivitäten zu verwischen. Die Ausführung des Wipers lenkte dadurch, mutmaßlich unbeabsichtigt, Aufmerksamkeit auf den bereits durchgeführten Sabotageakt und könnte auf einen Mangel an Koordination innerhalb des Angriffsteams hindeuten.

Mandiant schätzt, dass Sandworm mindestens drei Wochen vor dem letztlich erzielten Stromausfall in der Lage war, die für die Stromlieferung wichtigen OT-Systeme zu stören. Die tatsächliche Unterbrechung der Stromversorgung im Oktober durch den Eingriff in die Steueranlagen des Umspannwerks überschnitt sich mit einem mehrtägigen Raketenbeschuss auf kritische Infrastrukturen in der Ukraine, einschließlich der Stadt, in der das betroffene Energieunternehmen seinen Sitz hat.

In Anbetracht der Tatsache, dass Sandworm bereits die Möglichkeit hatte, die Operation vor diesem Raketenangriff durchführen, könnte die zeitliche Überlagerung auf Bemühungen hinweisen, den Einsatz von konventionellen Waffen mit Cyber-Fähigkeiten zu verbinden. Mit Blick auf Cyberoperationen bietet diese Kombination unter Umständen auch den Vorteil, die cyber-gestützte Ursache, wie in diesem Beispiel für den Stromausfall, zu vertuschen und die vorzeitige Entdeckung der Angriffswerkzeuge zu verhindern.

Regierungsstellen in den USA, dem Vereinigten Königreich und innerhalb der EU haben wiederholt klare Verbindungen zwischen Sandworm und dem Hauptzentrum für Spezialtechnologien (GTsST), auch bekannt als Einheit 74455, innerhalb des russischen Militärgeheimdienstes GRU gezogen.

Geographic distribution of operations



Brennpunkte und Zielmuster

Der am häufigsten im November 2023 betroffene Zielsektor war, wie auch schon im Vormonat, Unternehmen der Kritischen Infrastruktur mit 46 Fällen beziehungsweise 60% der neu aufgenommenen Fälle. Dies ist eine Steigerung zu den 39 Fällen im Oktober und deckt sich relativ gesehen mit den Vormonaten, abgesehen von einem Ausreißer nach unten im vergangenen Monat. Am zweithäufigsten betroffen waren in 25 Fällen (33%) staatliche Institutionen, was einen Rückgang von sieben Fällen oder 10 Prozentpunkte darstellt und damit auch in relativer Hinsicht unter den Vormonaten bleibt.

Bei einem Blick auf die betroffenen Staaten sind erneut die Vereinigten Staaten mit 23 Fällen am häufigsten betroffen, was wiederum 30% aller Vorfälle entspricht. Im Anschluss folgt Deutschland mit sieben Vorfällen und damit fast einem Drittel aller im November aufgenommenen Fälle, in den EU-Mitgliedsstaaten betroffen waren (insgesamt 18). Weiterhin häufig betroffen waren Japan mit fünf Vorfällen, Großbritannien und die Niederlande mit vier Vorfällen sowie Russland in drei Vorfällen mit Bezug zum Krieg in der Ukraine - dazu weiter unten noch genauer.

Im Bereich der kritischen Infrastruktur ist in diesem Monat mit elf Vorfällen der Gesundheitssektor am häufigsten betroffen, wobei in der öffentlichen Berichterstattung in den meisten Fällen sowohl unklar bleibt, wer hinter dem Angriff steht als auch, ob es sich um eine bekannte Ransomwaregruppe handelt. Bei der geographischen Verteilung fällt auf, dass dies in sieben Vorfällen US-amerikanische Gesundheitsdienste betroffen hat. Der Trend der letzten Jahre hin zu einer Zunahme von Angriffen im Gesundheitssektor hat nun die zuständige Behörde dazu veranlasst, eine originäre Cybersicherheitsstrategie in Aussicht zu stellen, die auch den Anstieg in Ransomware-Vorfällen berücksichtigen soll. Für Deutschland wurde für den Gesundheitsbereich ein Cybervorfall am Klinikum Esslingen aufgenommen, allerdings ohne bislang ersichtlichen Ransomwareeinsatz.

Weiterhin häufig betroffen bleiben unter den Kritischen Infrastrukturen die Telekommunikationsbranche sowie jene der "kritischen Fertigung" mit zehn bzw. neun Vorfällen. Für die Telekommunikationsbranche lässt sich eine gewisse Bandbreite feststellen, die von hacktivistischen Aktionen wie einem technisch wenig anspruchsvollen DDoS-Angriff auf die Webseite des Dienstleisters Cloudflare über den ebenfalls als "disruptiv" - mit höherer Intensität - aufgenommenen Angriff auf palästinensische Internetserver bis hin zu Datendiebstählen bei Vodafone in Spanien oder innerhalb der unten näher beschriebenen Aktion "Scarred Manticore", die auch Telekommunikationsunternehmen betroffen hat. Für den Bereich der kritischen Fertigung lässt sich die Mehrzahl der Fälle ähnlich wie im Gesundheitsbereich Ransomwaregruppen zuschreiben. Während im Gesundheitssektor das Interesse der kriminellen Akteure an besonders sensiblen personenbezogenen Daten ein Kernmotiv darstellt, ist dies im Bereich der kritischen Fertigung eher das Know-How der einzelnen Unternehmen gekoppelt. Im November betraf dies etwa den Flugzeughersteller Boeing, den japanischen Elektronikhersteller Sony oder den niederländischen Chiphersteller NXP.

Bei den staatlichen Institutionen bleiben sowohl "Civil Service/Administration" mit elf und "Government/Ministries" zehn Vorfällen mit Abstand am häufigsten betroffen. Für Civil Service zeigt sich mit zwei Schwerpunkten bei Bildungseinrichtungen (darunter der British Library) und lokalen Institutionen wie mehrere Gemeinden im Landkreis Neu-Ulm, der Stadt Neuss oder der Schweizer Gemeinde Zollikofen ein bekanntes Bild, wobei sich die tatsächlichen Auswirkungen im Einzelnen doch unterscheiden und gewisse Vorurteile widerlegen: So ist die längste Beeinträchtigung von IT-Systeme für die British Library aufgenommen.
Für Government/Ministries lassen sich den Konflikten in der Ukraine bzw. in Israel auch im November einige DDoS-Angriffe zuordnen, die etwa die Webseiten schweizerischer, belgischer sowie Regierungsinstitutionen Bahrains trafen. Ebenfalls mutmaßlich politisch motiviert sind die Angriffe mehrerer dem chinesischen Staat zugeschriebener APTs auf Regierungsbehörden in Kambodscha und den Philippinen zu betrachten, die vermutlich jeweils Spionagezwecke verfolgten.

Angreiferprofile und Attributionen

Auch im November konnte ein Großteil der erfassten Cyberoperationen (bislang) keinem Ursprungsland der Verantwortlichen zugesprochen werden, so blieb in 70 Prozent der Fälle (53) die Urheberschaft noch unklar, was abermals in etwa dem 70%-Durchschnitt dieses Werts der Vormonate entspricht. In 25 der 76 Fälle wurden nicht staatliche Akteure verantwortlich gemacht, was nur knapp 3% weniger als im Vormonat Oktober entspricht. Von den 25 Fällen wurden in 14 kriminelle Gruppierungen als Täter identifiziert, bzw. reklamierten diese die Hacks zumeist für sich, etwa im Rahmen von Ransomware-Vorfällen (14 der 14 Fälle). Die übrigen 11 Fälle nichtstaatlicher Akteure waren dagegen stärker politisch-ideologisch motiviert. Diese relative Verteilung entspricht in etwa der des Vormonats Oktober. Wie in den Monaten zuvor auch schon, dominieren sowohl bei kriminell als auch politisch motivierten Hacks Gruppierungen mit russischen Verbindungen, etwa auf Seiten der Hacktivisten auch im November wieder durch diverse Operationen der Gruppe NoName057(16) (3 DDoS-Vorfälle). Gleiches gilt für die kriminelle Ransomware-Gruppe Lockbit, ebenfalls mit drei attribuierten Vorfällen im November.

Die Liste attribuierter Herkunftsländer der Angreifer zeichnet sich im November durch eine geringere Anzahl / Diversität aus, etwa im Vergleich zum Monat September, in dem zehn unterschiedliche Länder identifiziert werden konnten. Weniger überraschend ist dagegen, dass auch im November mal wieder die “üblichen Verdächtigen” in dieser reduzierten Liste zu finden sind: Russland, Nordkorea, Iran und China - aber auch die Ukraine, aufgrund der Einbindung nichtstaatlicher sowie staatlicher Akteure in regelmäßigen Cyberkonfliktaustrag mit Russland.

Auf Seiten der sogenannten “Cyberproxies”, also von Staaten geduldete oder beauftragte Hackergruppierungen, bei denen jedoch die tatsächliche Abtrennung von staatlichen Stellen auch zunehmend verschwimmen kann, wurden im November sechs Vorfälle erfasst. Drei davon für iranische Gruppen, zwei für nordkoreanische Stellvertreter, und ein Fall chinesischer Proxy-Tätigkeiten. Für den Iran sticht der Spionagefall der von CheckPoint Security unter dem Namen “Scarred Manticore” dokumentierte Gruppe hervor, da diese zuvor noch kein Gegenstand ausführlicher Threat Intelligence Berichte war.

In dem betreffenden Fall erlangte die Gruppe, der Verbindungen zum iranischen Ministry of Intelligence and Security (MOIS) nachgesagt werden, Zugang zu den Windows Servern verschiedener staatlicher und privater Institutionen des Mittleren Ostens, unter der Verwendung des LIONTAIL Malware Frameworks, seit mindestens 2022. Auch wenn Scarred Manticore eher als Spionageakteur beschrieben wird, konnte CheckPoint eine Verbindung zu vorherigen, disruptiven iranischen Operationen der letzten Zeit ziehen: so werden einige der von Scarred Manticore verwendeten Werkzeuge mit den destruktiven Angriffen gegen die albanische Regierungsinfrastruktur Mitte Juli 2023 assoziiert. Da auch hierfür jedoch von Microsoft unterschiedliche Akteure für unterschiedliche Phasen der Operationen verantwortlich gezeichnet wurden, bleibt offen, ob es sich hier lediglich um ein unter nationalen APTs immer üblicheres Tool-Sharing handelt, oder ob Scarred Manticore womöglich auch schon in die Operationen gegen Albanien involviert war. Der Fall verdeutlicht die seitens Iran seit nunmehr vielen Jahren umfassend betriebene, geopolitisch motivierte Cyberspionage. Verantwortlich dafür zeichnen sich staatlich

gelenkte, oder zumindest beauftragte Gruppierungen, die laut Threat-Intelligence-Erkenntnissen in einem immer weiter gedeihenden Ökosystem um staatliche Aufträge konkurrieren, weshalb in der Vergangenheit auch bereits offiziell kommerzielle oder wissenschaftliche Institutionen, wie das Mabna-Institut, als iranische Cyberproxies entlarvt wurden. Dabei können die Gruppierungen zumeist entweder den Revolutionsgarden, oder dem erwähnten MOIS zugeordnet werden.

Dass staatliche Stellen eines Landes offiziell zugeben, Ziele eines anderen gehackt zu haben, bildet eine deutliche Ausnahme. In der Vergangenheit gab es zwar seitens der USA in Einzelfällen Aussagen zu eigenen Cyberoperationen, wie etwa gegen die Internet Research Agency aus St. Petersburg als Präventivmaßnahme vor den Midterm-Elections 2018, oder auch via Medien-Berichte durchgestochene Aussagen zu Cyberoperationen gegen iranische Ziele im Rahmen von Spannungen in der Straße von Hormus 2019. Dass ein militärischer Geheimdienst, wie eingangs für den Fall der ukrainischen Spähoperation gegen Rosaviatsia beschrieben, auf der eigenen Website eine Hack-and-Leak-Operation selbst bekannt und hierzu auch noch umfassende Informationen preisgibt, war so bis dato noch nicht vorgekommen. Diese Daten sollen zeigen, wie schwer die dem Land auferlegten Sanktionen der russischen Luftfahrt auch im Zivilbereich zusetzen, diese stehe kurz vor dem “Kollaps”. Offizielle ukrainische Verlautbarungen anhand der erbeuteten Dokumente, wonach die Russland auferlegten Sanktionen auch der zivilen Luftfahrt zusetzen, wurden im Laufe des Dezembers von weiteren Medienberichten bekräftigt. Hack-and-Leak-Operationen verfolgen eigentlich das Ziel, hinter dem Schleier der “plausible deniability” Einfluss auf innere Prozesse eines fremden Landes nehmen zu können, etwa im Vorfeld von nationalen Wahlen. Dabei wird die eigene Täteridentität nicht offen gelegt, hat dies doch den Vorteil, dass der öffentliche Fokus auf den Inhalten der zumeist kompromittierenden Leaks verbleibt, wie geschehen im Falle der russischen Störung der US-Wahlen 2016. Zum anderen sind sich gerade staatliche Täter des eigenen Normbruchs wohl bewusst, da man mit solchen Cyberoperationen in Friedenszeiten aus völkerrechtlicher Sicht durchaus die Souveränität eines anderen Landes verletzen und gegen das sogenannte “Nicht-Interventionsverbot” verstoßen kann. Im Rahmen eines internationalen bewaffneten Konflikts, wie in der Ukraine, tritt das humanitäre Völkerrecht an die Stelle dieser Erwägungen, das unter anderem einen besonderen Schutz ziviler Infrastruktur verlangt. Dass sich die Ukraine ganz offen zu einer solchen Handlung bekennt, liegt vermutlich vor allem an drei Gründen: Erstens empfindet sie ihr Vorgehen aufgrund der russischen Aggressionen, die die Kampfhandlungen ja erst begründeten, nicht als illegitim, sondern als notwendig und gerechtfertigt im Rahmen ihrer Selbstverteidigung. Zweitens möchte sie mit ihrer Hack-and-Leak-Operation vermutlich auch ganz bewusst die russische Bevölkerung ansprechen, um ihr die negativen Folgen des Angriffskriegs des Kremls auf ihre eigene persönliche Sicherheit aufzuzeigen. Drittens könnte das Vorgehen auch als ein bewusstes Signal an die eigenen Verbündeten gewertet werden, um ihnen den Nutzen der verhängten Sanktionen zu vergegenwärtigen und ihre andauernde Unterstützung somit weiterhin zu gewährleisten.

Die Attribution, die auch vor dem Hintergrund der erwähnten Grenzen des humanitären Völkerrechts die größte Aufmerksamkeit im November erhalten hat, war der bereits erwähnte Bericht von Mandiant zu einer disruptiven Wiper-Operation der russischen Militärgeheimdienst-Hackergruppe Sandworm gegen ukrainische kritische Infrastrukturen im Energiesektor im Oktober 2022.

Wie schon zuvor im Oktober dominierten im November die Konflikte zwischen der Ukraine und Russland (10 Vorfälle), sowie der Hamas und Israel (3 Vorfälle) bei den Cyberoperationen, die das Repositorium bestehenden konventionellen Konflikten, erfasst im Konfliktbarometer des Heidelberger Instituts für Internationale Konfliktforschung, zuordnen konnten (insgesamt 15 von 76). Ein weiterer Fall betrifft die Iran-Israel Konfliktdyade. Ein mutmaßlicher Cyberspionagefall der chinesischen APT Mustang Panda gegen philippinische Regierungssysteme im August 2023 ist dem übergeordneten Konflikt zahlreicher Länder um das südchinesische Meer zugerechnet. Dem Vorfall war ein Aufeinandertreffen der chinesischen Küstenwache mit einem philippinischen Schiff unmittelbar vorausgegangen.
Auch wenn Cyberoperationen u.a. den Vorteil bieten, dass man für ihre Durchführung zumeist keine physische Präsenz in den Zielländern mithilfe von Agenten aufbauen/unterhalten muss, zeigen die drei genannten Konfliktdyaden, dass unterschiedliche Cyberoperationsformen besonders auch im Rahmen regionaler Konflikte mit variierenden Zielsetzungen zum Einsatz kommen, u.a. in Abhängigkeit vom jeweiligen Eskalationsstatus des Konflikts.

Mehr von EuRepoC

Als dritten Cyber Information Tracker, neben dem zu abonnierenden täglichen Cyber Incident Tracker sowie dem EU Media Tracker, bietet EuRepoC nun auch einen Attribution Tracker auf der Projektwebseite an. Dieser liefert auf monatlich aktualisierter Basis quantitative und qualitative Zahlen und Einordnungen zu den im Datensatz erfassten Attributionen der letzten sechs Monate. Die Daten werden jeden Monat aktualisiert, um so kurz- und langfristige Attributionstrends auf europäischer und internationaler Ebene identifizieren zu können.

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 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).