European
Repository of
Cyber Incidents

EuRepoC

Cyber Conflict Briefing

September 2023

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

Beobachtungen zur Gesamtlage

Im **September 2023** wurden 86 Cyber-Operationen in die EuRepoC-Datenbank aufgenommen. Das sind 37% mehr als im Vormonat, und 30 Operationen mehr als die insgesamt durchschnittlich verzeichnete Aktivität von 56 Cyber-Operationen pro Monat im Gesamtzeitraum.

Die **durchschnittliche Intensität** der im September 2023 erfassten Operationen beträgt 2,5 und liegt somit unter 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 September stattgefunden haben, sondern können bereits zu einem früheren Zeitpunkt begonnen haben. Dabei stehen technische, politische sowie rechtliche Aspekte im Vordergrund.

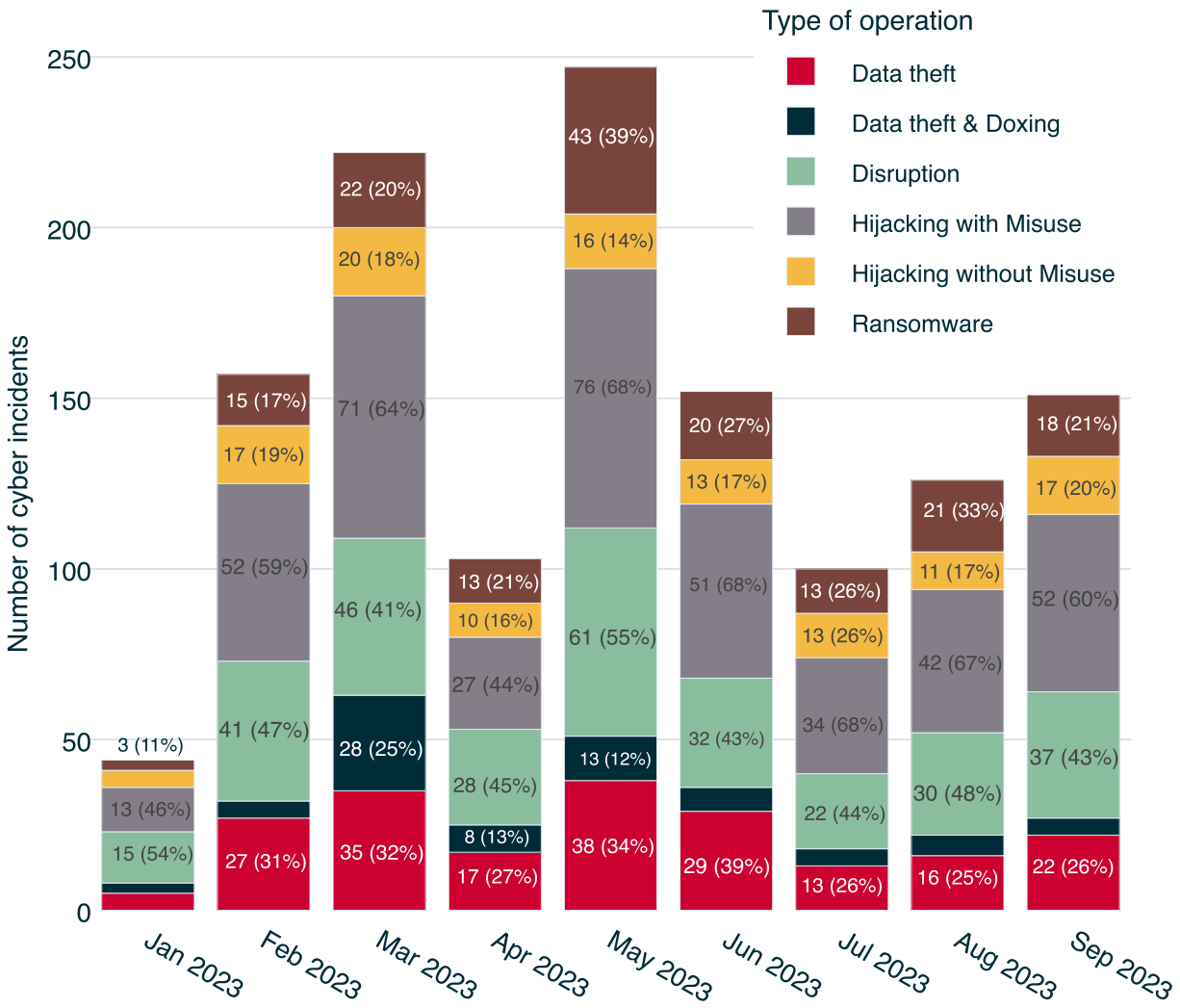
Über EuRepoC

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 September 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 (60%). 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. Steigend vertretene Operationen betreffen den Diebstahl von Kryptowährungen. Anfang September führte das FBI die Entwendung von umgerechnet 41 Millionen US-Dollar von der Online-Kasino- und Wettplattform Stakes.com auf staatliche Akteure aus Nordkorea zurück.

Konkret machen Angaben des FBI die Lazarus-Gruppe für den Raub verantwortlich mit weiterem Verweis auf APT38. Beobachtungen aus den der Gruppe zugerechneten Aktivitäten und eingesetzten Werkzeugen legen nahe, dass es sich bei Lazarus um ein Netzwerk von Akteuren handelt, das als Teil des nordkoreanischen Generalbüros für Aufklärung innerhalb der Nordkoreanischen Volksarmee agiert. Einheiten mit Lazarus-Verbindung arbeiten insbesondere im auf ausländische Erkenntnisgewinnung spezialisierten dritten Büro.

Eine dieser Einheiten ist APT38, die mit besonderem Schwerpunkt auf Ziele im Finanzmarktbereich operiert. Das Threat-Intelligence-Unternehmen Mandiant dokumentierte im Oktober 2023 eine seit längerem anhaltende operative Pause für APT38. Aktiv sind Untergruppen, wie CryptoCore (UNC1069) und TraderTraitor (UNC4899), die sich auf den Diebstahl von Kryptowährungen konzentrieren und laut Mandiant mutmaßlich durch Angehörige von APT38 verstärkt wurden. Die Verknüpfung von bestimmten Aktivitäten mit einzelnen Subgruppen sowie die Unterscheidungen zwischen den Operationsprofilen von Untereinheiten bleibt eine Herausforderung, unter anderem weil nordkoreanische Operateure aufgrund ihrer Einordnung in militärische Strukturen von gemeinsamen Standorten arbeiten.

Die FBI-Bekanntmachung von September führt die Verweise auf Lazarus und APT38 synonym. Eine vorausgehende Meldung des FBIs im August identifizierte TraderTraitor im Zusammenhang mit einer Reihe von Diebstählen während der Sommermonate, setzte diese Untergruppe jedoch ebenfalls gleich mit Lazarus und APT38 ohne genauere Angaben zu einer eventuellen begrifflichen Unterscheidung.

Bisher zeichnete sich APT38 für die größten Diebstähle verantwortlich, wie unter anderem den Raub von fast einer Milliarde Dollar von einem Konto der Zentralbank Banladeschs 2016 durch betrügerische Anweisungen, die über SWIFT verschickt wurden, ein Netzwerk, das Finanztransaktionen zwischen Banken vermittelt. APT38 sticht vor allem durch die Bereitschaft heraus, Daten in kompromittierten Netzwerken zu löschen, um eventuelle Hinweise auf die eigenen Operationen zu verwischen.

Insgesamt haben nordkoreanische Gruppierungen Stand Mitte September 2023 nach Schätzungen 340,4 Millionen US-Dollar in Kryptowährung erbeutet – mit der Aussicht die Zahlen der meisten vergangenen Jahre zu übertreffen.

Der zweithäufigste im September 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. Davon sind 37 durch das Repositorium erfasst. Störungen dieser Art stellen eine mögliche Ausprägung von Ransomwareattacken dar. Mitte September führte ein so verursachter Ausfall von datenabhängigen Diensten mehrerer Regierungsbehörden in Kolumbien zu Unterbrechungen von gerichtlichen Verfahren und Beeinträchtigungen in der medizinischen Versorgung.

Unmittelbares Ziel war das in den USA ansässige Telekommunikationsunternehmen IFX Networks – ein Internet-Provider und der führende Anbieter von public-private Cloudlösungen in Lateinamerika. Dort verhinderte der Einsatz von Ransomware das reguläre Bereitstellen von hinterlegten Kundendaten. In Kolumbien waren neben anderen staatlichen Stellen insbesondere das Gesundheitsministerium, die Aufsichtsbehörde des Gesundheitswesens und Justizorgane durch ihre Abhängigkeit von IFX Datenzentren von betriebswichtigen Informationen abgeschnitten.

Einschränkungen betrafen die Möglichkeit, Arzttermine zu vereinbaren, und den Zugriff auf Krankenakten. Verzögerungen in der Bearbeitung von Gerichtsverfahren machten zudem eine mehrwöchige Aussetzung von Prozessfristen nötig. Nach Aussage des in Kolumbien für das Krisenmanagement in diesem Fall zuständigen Berater des Präsidenten hätten die verantwortlichen Kriminellen außerdem Zugriff auf die Informationen von mehreren Millionen Menschen erhalten.

Die weitreichenden Unterbrechungen verdeutlichen potentielle Clusterrisiken auf, die durch den konzentrierten Einsatz einzelner Cloudlösungen im Fall mangelnder Vorsorge der Anbieter begünstigt werden können.

Insgesamt beeinträchtige der Eingriff in die IFX-Rechencenter 619 Organisationen und über 6000 Dienstleistungen, unter anderem in Chile und Argentinien. Das zuständige Reaktionszentrum des kolumbianischen CSIRTs erfüllte 35 Unterstützungsanfragen, 20 von Firmen und 15 aus dem öffentlichen Sektor.

Vor diesem Hintergrund prüft die kolumbianische Regierung rechtliche Schritte und untersucht, ob der Provider den gemachten Cybersicherheitsauflagen entsprochen hat.

Brennpunkte und Zielmuster

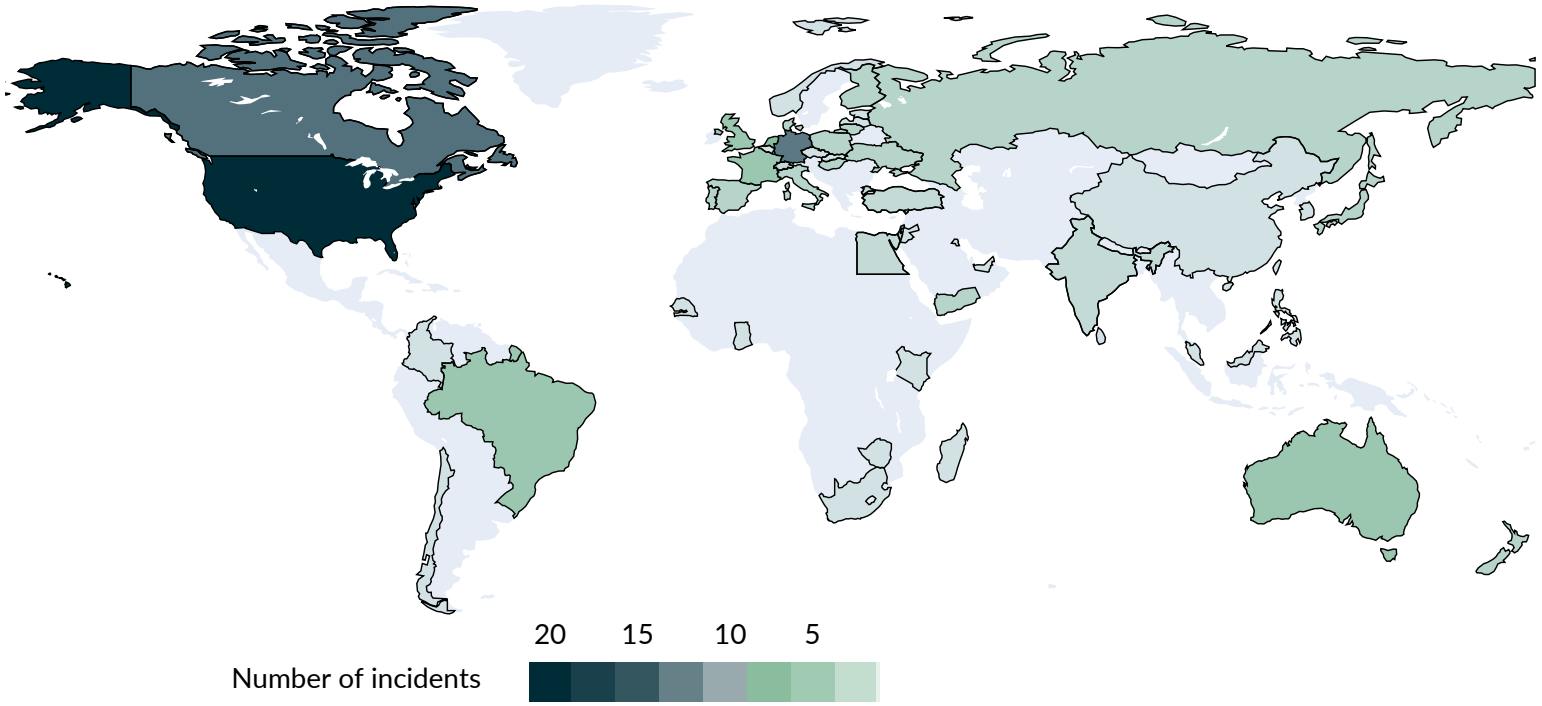
Der am häufigsten im September 2023 betroffene Zielsektor war, wie auch schon im Vormonat, Unternehmen der Kritischen Infrastruktur mit 50 Fällen beziehungsweise 58% der neu aufgenommenen Fälle. Dies stellt einen Anstieg um fast 40% im Vergleich zu den 36 Fällen im August dar. Am zweithäufigsten betroffen waren in 42 Fällen (49%) staatliche Institutionen.

Dies stellt gegenüber dem August mit 26 Fällen eine merkliche Steigerung um mehr als 60% dar. In Relation zu den Vormonaten macht sich dies ebenso bemerkbar: Während in den Vormonaten etwa drei von fünf Cybervorfällen kritische Infrastrukturen betrafen, war dies für staatliche Institutionen bisher nur in zwei von fünf Vorfällen der Fall.

Bei einem Blick auf die betroffenen Länder zeigen sich die Vereinigten Staaten mit 19 Vorfällen weiterhin am stärksten betroffen. Im Anschluss daran folgt mit Deutschland (11 Vorfälle) der erste EU-Mitgliedsstaat, eine merkliche Steigerung gegenüber den “ruhigeren” Sommermonaten. Weiterhin häufig betroffen waren Kanada mit acht, die Niederlande mit sieben und Australien mit fünf Vorfällen. Entgegen der Vormonate fand eine merkliche Verschiebung in relativer Hinsicht statt. So waren die Vereinigten Staaten nur mehr in 23% statt circa 30% aller Vorfälle betroffen, während die Zahl der EU-Mitgliedsstaaten betreffenden Vorfälle auf dem im letzten Monat beobachteten 30%-Niveau blieb, was weiterhin eine Steigerung gegenüber dem Vormonat darstellt.

Ein Blick über die betroffenen Infrastruktursektoren zeigt ein teils bekanntes, teils neues Bild: Für den Juli registrierte EuRepoC zum ersten Mal den Finanzsektor als am häufigsten betroffenen Infrastrukturzweig in der monatlichen Zurückschau. Diese Beobachtung wiederholte sich nun in kurzer Folge im September (elf Vorfälle). Fünf der Vorfälle betrafen Kryptohandelsplattformen, wobei Dienste aus China beziehungsweise Hongkong (hier und hier), Kanada sowie den Seychellen betroffen waren.

Geographic distribution of operations



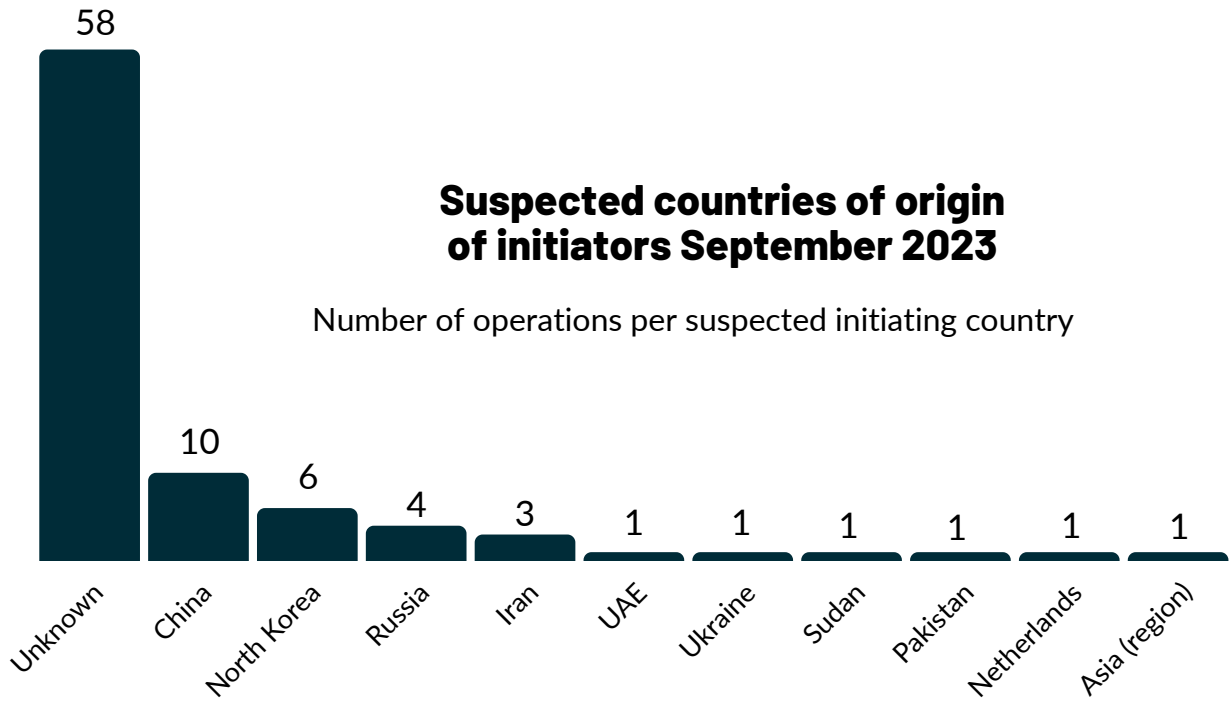
Anders als für viele andere Cybervorfälle, in denen die Schadenssummen nur schwierig zu ermitteln sind und deshalb häufig auf gemittelten Schätzungen beruhen, ist dies für Kryptobörsen angesichts der transparenten Blockchain-Technologie einfacher - allein für den September liegt der momentane Schaden bei über 240 Millionen. US-Dollar. Im Finanzbereich war für Deutschland der Diebstahl personenbezogener Daten bei der Sparkassentochter Deutsche Leasing relevant.

Weiterhin häufig betroffen bleibt der Gesundheitssektor, für den im September neun Vorfälle in das Repositorium aufgenommen wurden. Hier scheint es in einer Mehrzahl der Fälle wahrscheinlich, dass keine spezifische Auswahl an Zielen erfolgt ist, sondern es sich um Spray-and-Pray-Angriffe handelt. Ähnliches liegt auch für einen Großteil der restlichen aufgenommenen Vorfälle im Finanzbereich nahe.

Für den ebenfalls mit neun Vorfällen betroffenen Telekommunikationssektor lässt sich ebenfalls kein eindeutiges Bild erkennen.

So lassen sich manche Vorfälle etwa dem Ziel der Cyberspionage zuordnen, wie etwa das Vorgehen der Gruppen “BlackTech” gegen US-amerikanische und japanische Konzerne oder “Sandman”. Andere wiederum stellen sich als klassische Ransomwareoperationen dar. Und zuletzt zeigten die erwähnten Auswirkungen der Ransomwareattacke gegen IFX Networks in Kolumbien, welche Gefahren von Anbieterabhängigkeiten auch für staatliche Institutionen ausgehen können.

Für diese Institutionen zeigt sich weiterhin, dass die unter ‘Civil service/administration’ geführten 27 Vorfällen bei sub-nationalen Behörden mit fast zwei Dritteln erneut die Mehrzahl der Vorfälle bei öffentlichen Einrichtungen darstellen. Wie in den vergangenen Monaten lässt sich dies auf das insgesamt wohl niedrigere Cybersicherheitsniveau zurückführen. In Deutschland war dies etwa ein DDoS-Angriff auf die Seite des Landes Berlin oder Vorfälle an Bildungseinrichtungen wie der Hochschule Furtwangen sowie dem Helmholtz-Gymnasium in Zweibrücken.



Auf nationaler Ebene betroffen war die Finanzaufsichtsbehörde BaFin durch einen weiteren DDoS-Angriff sowie ein erst jetzt bekannt gewordener Hack beim Bundesamt für Kartographie und Geodäsie im Jahr 2021.

Angreiferprofile und Attributionen

Auch im September pendelte sich der Prozentsatz der (noch) nicht konkreten Angreiferländern zugeordneten Cybervorfälle (Anzahl: 58) mit 67% um die 70% Marke ein. In 27 der 86 Fälle wurden nichtstaatliche Akteure verantwortlich gemacht, was prozentual einen Rückgang von ca. 12% im Vergleich zum Vormonat August bedeutet. Für 20 der 27 Fälle zeichneten sich kriminelle Akteure verantwortlich, lediglich in einem Fall wurde hier mit Russland ein Ursprungsland erfasst. Dies unterstreicht einmal mehr den erstens oftmals transnationalen Charakter der immer professioneller agierenden Hacker-Kollektive sowie zweitens die Schwierigkeiten der Attribution potenziell bestehender Verbindungen der Gruppen zu konkreten Staaten.

In den verbleibenden sieben Fällen reklamierten politisch motivierte Hacktivisten die Vorfälle für sich, mit jeweils einer Attribution der Ursprungsländer Ukraine, Russland, Pakistan und Sudan. Letztere Attribution wurde jedoch als umstritten gekennzeichnet, handelte es sich doch um einen weiteren DDoS-Fall der Gruppierung Anonymous Sudan, die in der Vergangenheit seitens Threat Intelligence Unternehmen als False-Flag-Operation der russischen Gruppe KillNet bezeichnet wurde. In dem vorliegenden Fall reklamierte die Gruppe die Blockade des Zugangs zum Social Media-Netzwerk X für etwa zwei Stunden für sich. Laut der Gruppe bezweckte sie mit der Aktion, Elon Musk dazu zu bringen, sein Satelliteninternet Starlink künftig auch im Sudan anzubieten sowie auf die dortige Situation im Bürgerkrieg aufmerksam zu machen. Elon Musk`s Rolle als CEO einer Firma, die es Ländern ermöglicht, unabhängig von Unterseekabeln Internetzugang zu beziehen, impliziert somit nach wie vor erhebliche (geo-)politische Sprengkraft, auch über die Ukraine hinaus.

Erst Anfang September war bekannt geworden, dass Musk ein Jahr zuvor der Ukraine verweigert hatte, Starlink für einen militärischen Überraschungsangriff auf die Krim zu nutzen, da er befürchtete, sich somit mitverantwortlich für eine weitere Eskalation des Krieges zu machen. Musk`s Unternehmen SpaceX hatte der Ukraine sein Produkt Starlink auf eigene Kosten sowie über eine Vereinbarung mit der U.S. Agency for International Development (USAID) zur Verfügung gestellt, nicht aber im Rahmen eines Vertrages mit dem U.S. Verteidigungsministerium. Die gestiegene Brisanz der Rolle des Privatsektors im Rahmen bewaffneter Konflikte reflektierten auch jüngst die vom Komitee des Internationalen Roten Kreuzes veröffentlichten Empfehlungen an Technologieunternehmen, wie diese Zivilisten darin vor digitalen Bedrohungen schützen können.

In 17 der 86 Fälle im September wurden Cyber-Proxies als verantwortliche Akteure benannt, was etwa sechs Prozent mehr sind als im August. Von den 17 Fällen wurden sieben China als Sponsor-Land, sechs Nordkorea, drei dem Iran und ein Fall den Vereinigten Arabischen Emiraten zugesprochen. Auch im August zeichnete sich China für die meisten Proxy-Operationen verantwortlich. Im September führt das Land zudem die Gesamtliste der attribuierten Angreifer-Herkunftsländer mit zehn Vorfällen vor Nordkorea, Russland und dem Iran an. Diese Vierergruppe bildet ein konstantes Gefüge, auch wenn die jeweiligen Platzierungen von 1-4 über Zeit variieren können. Im Falle Nordkoreas spiegeln die erfassten sechs Proxy-Operationen die grundlegenden Motivlagen des Regimes in Pjöngjang zur Durchführung von Cyberoperationen wider: vier davon fokussierten sich auf Datendiebstahl der Rüstungsindustrie (u.a. in Deutschland und Israel) und Wissenschaft (Forschungsinstitut für Luft- und Raumfahrt in Russland), mutmaßlich um das eigene Atomwaffenprogramm als zentrales Abschreckungspotenzial weiter zu stärken. Die verbliebenen zwei Fälle betrafen dagegen den Finanz- und Kryptowährungssektor, ebenfalls um die eigene Regimesicherheit trotz bestehender internationaler Sanktionen kräftigen zu können. Cyberoperationen können besonders digital abgeschotteten Ländern wie Nordkorea einen asymmetrischen Vorteil verschaffen, indem sie die bestehenden Interdependenzen demokratischer Länder im Cyberspace erst zu Verwundbarkeiten machen.
Auf Seiten Chinas stechen unter den sieben Proxy-Operationen vier Kompromittierungen staatlicher Entitäten aus der unmittelbaren asiatischen Nachbarschaft heraus, mit dem mutmaßlichen Ziel der Cyberspionage. Auch wenn vor allem die People`s Liberation Army (PLA) in den letzten Jahren im Rahmen geopolitischer Konflikte wie mit Indien oder Staaten am südchinesischen Meer immer stärkere Fähigkeiten zu militärisch orientierten Cyberoperationen entwickelt hat (siehe hierzu auch der kürzlich erschienene Jahresbericht des US Verteidigungsministeriums), liegt der chinesische Fokus nach wie vor auf dem Diebstahl von Daten. Diese können geistiges Eigentum, Staatsgeheimnisse, aber auch kompromittierende Daten von RegimegegnerInnen betreffen.
Die Zahl der dem russischen Krieg gegen die Ukraine zugeordneten Operationen fällt im Vergleich zu den Vormonaten leicht ab (3), konstant blieb jedoch die Präsenz der Hacktivisten-Gruppe NoName057(16), die für zwei davon verantwortlich war.
Auch im September berichteten Threat Intelligence Unternehmen über zuvor unbekannte Gruppierungen.

So veröffentlichten SentinelOne und QGroup gemeinsam einen Bericht über ein zuvor noch nicht diskutiertes "Aktivitätscluster", welchem sie den Namen "Sandman" gaben. Die Gruppe habe im August 2023 Telekommunikationsanbieter in Europa, Südasien und im Nahen Osten ausspioniert und sei womöglich ein privater Vertragsnehmer, da einerseits zwar keine Verbindungen zu einem konkreten Staat, andererseits jedoch klare Prioritäten der Spionage beobachtet werden konnten. Denkbar ist, dass im Laufe der Zeit bei wiederholten Operationen der Gruppierung zusätzliche Evidenzen Aufschluss darüber liefern, ob und falls ja, zu welchem Staat die Gruppe womöglich doch engere Verbindungen unterhält oder durch diesen gar komplett gesponsert oder gesteuert wird.

Als zweiter "Newcomer" wurde im September vom japanischen Threat Intelligence Unternehmen TrendMicro die Gruppierung "Earth Estries" öffentlich gemacht, welche insgesamt seit 2020 operativ tätig sein soll. Im betreffenden Fall hatte sie seit mindestens Anfang 2023 Regierungen und Technologie-Unternehmen in u.a. Deutschland, Taiwan, Philippinen, Malaysia, Südafrika und USA mit Hilfe der Backdoor Zingdoor, dem TrillClient Information Stealer, sowie der HemiGate Backdoor ausspioniert. Laut TrendMicro lassen sich aufgrund der beobachteten TTPs Verbindungen zur Gruppierung FamousSparrow ziehen, welche laut dem Threat Intelligence Unternehmen ESET seit mindestens 2019 aktiv ist.

Auf Seiten der Attributionen rückt im September ein - wenn es um Cyberangriffe geht - ansonsten eher wenig thematisiertes Land in den Mittelpunkt: Bermuda. Am 21. September hatte der Premierminister David Burt im Rahmen einer Pressekonferenz mitgeteilt, dass mutmaßliche Angreifer aus Russland weite Teile der staatlichen IT-Infrastruktur lahm gelegt hätten.

Nachdem der Verlauf der Pressekonferenz ein besonderes Interesse der anwesenden JournalistInnen an dem Vorfall offenbarte, folgte bereits einen Tag später eine weitere, explizit dem Vorfall gewidmete Ansprache des stellvertretenden Premierministers Walter Roban. Darin unterstrich er vor allen Dingen die Bemühungen der Administration, die Folgen des Vorfalls einzugrenzen und versicherte der Bevölkerung unter Anderem, dass keine zentralen Notfalldienste betroffen seien ("911"). Gerade im September befindet sich Bermuda mitten in der Hochphase der Hurrikan-Saison, weshalb das ungestörte Funktionieren dieser Kommunikationssysteme, sowie das öffentliche Vertrauen darin von besonderer Wichtigkeit ist. Die Reaktion der Regierung Bermudas auf den Vorfall war in jedem Falle auffallend proaktiv und zeitnah, auch wenn bislang keine weiteren Details zu der Attribution in Richtung Russland veröffentlicht wurden.

Mehr von EuRepoC

In einem Ende September veröffentlichten SWP-Podcast diskutieren Annegret Bendiek und Jakob Bund die immer ausgefeilteren Methoden von Angreifern im Cyberspace und wie politische EntscheidungsträgerInnen hierauf am effektivsten reagieren können.

Eine neue Ausgabe der EuRepoC-“Major Cyber Incident Profiles” (MACIs) behandelt mit KA-SAT 9A den bislang disruptivsten Wiper-Angriff im Rahmen des russischen Krieges gegen die Ukraine, der auch in Deutschland zu Störungen bei Unternehmen führte.

Im Rahmen des Redesigns der EuRepoC-Website stellt das Repositorium ab sofort eine erweiterte interaktive Version des EU Media Reporting Trackers, mit monatlich aktualisierten Daten zur Medien-Berichterstattung über Cybervorfälle in der EU, zur Verfügung.

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 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).