European
Repository of
Cyber Incidents

EuRepoC

Cyber Conflict Briefing

Oktober 2023

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

Beobachtungen zur Gesamtlage

Im **Oktober 2023** wurden 79 Cyber-Operationen in die EuRepoC-Datenbank aufgenommen. Das sind 8% weniger als im Vormonat, aber 21 Operationen mehr als die insgesamt durchschnittlich verzeichnete Aktivität von 58 Cyber-Operationen pro Monat im Gesamtzeitraum.

Die **durchschnittliche Intensität** der im Oktober 2023 erfassten Operationen beträgt 2,36 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 Oktober stattgefunden haben, sondern können bereits zu einem früheren Zeitpunkt begonnen haben. Dabei stehen technische, politische sowie rechtliche Aspekte im Vordergrund.

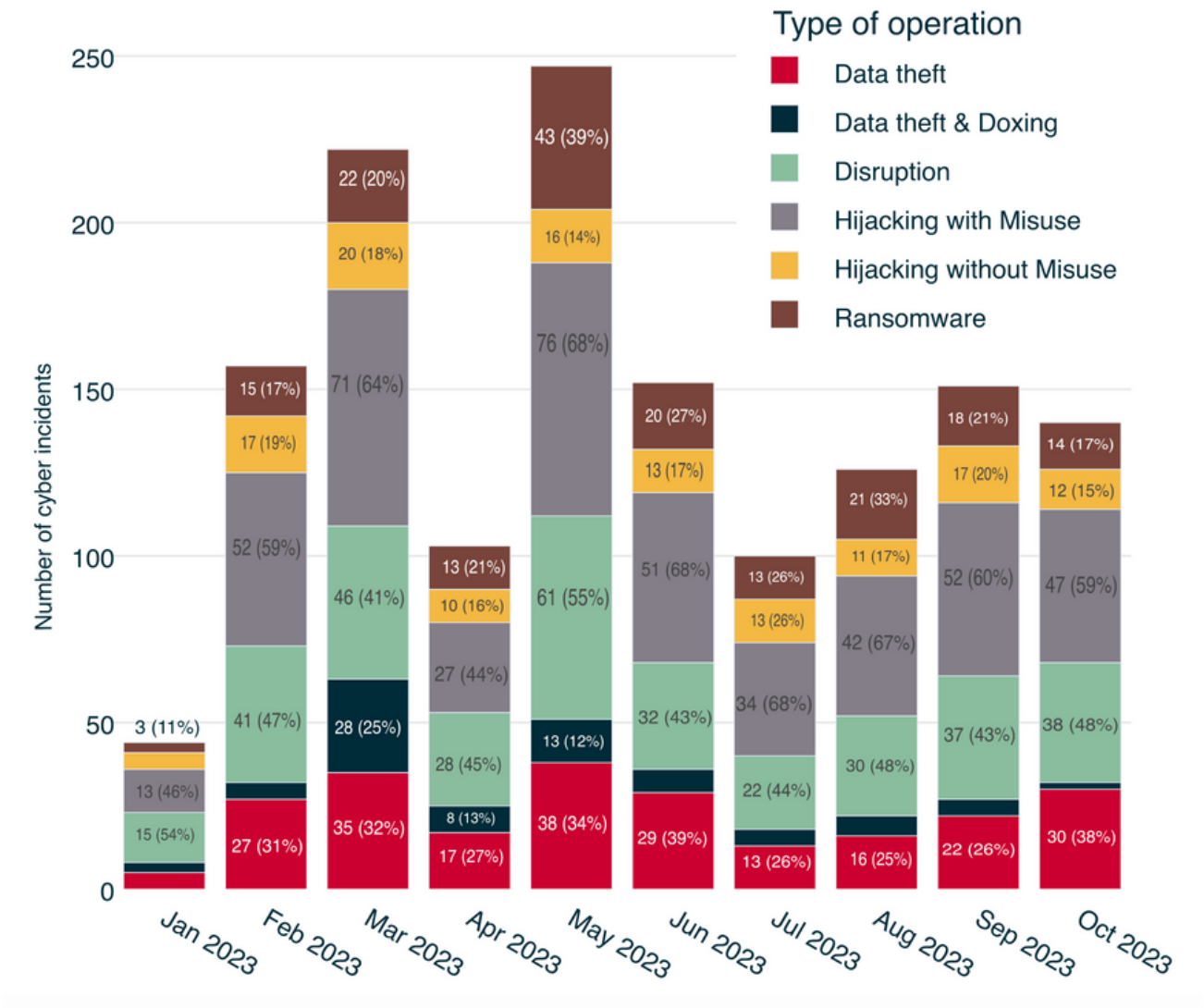
Über EuRepoC

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 Oktober 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 47 Fällen (59%). 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.

Analysen von Kaspersky zeigen genau diese Schwierigkeit in der Deutung von Motiven und der strategischen Einordnung solcher Operationen. Mehr als fünf Jahre nach der ersten Entdeckung eines vermeintlichen Cryptominers weisen Erkenntnisse von Sicherheitsforschende der Firma auf verdeckte Spionageziele der Schadsoftware hin. Codebestandteile der Malware StripedFly zeigen Parallelen zu Werkzeugen der Equation Group, hinter welcher der US-amerikanische Geheimdienst NSA vermutet wird.

Die zunächst entdeckte Cryptominer-Fähigkeit sollte mutmaßlich weitere Module verschleiern. Unter anderem setzt die Schadsoftware einen Exploit mit hoher Ähnlichkeit zu EternalBlue ein, der eine Schwachstelle im Netzwerk-Protokoll SMBv1 ausnutzt, um sich nahezu ungehindert weiterzuverbreiten. Nach Beobachtungen von Kaspersky wurden Elemente des Exploits zuletzt am 22. April 2023 aktualisiert. Versteckte Module enthalten Fähigkeiten, Zugangsdaten auszuspähen, Screenshots und Tonaufnahmen zu machen sowie weitreichende Informationen über kompromittierte Systeme zu sammeln.

Der vermutete hohe Stellenwert von Heimlichkeit für StripedFly leitet sich ebenfalls von besonderen Anstrengungen ab, die Verbindungen zum Command-and-Control-Server zur Steuerung dieser Fähigkeiten vor einer Offenlegung zu schützen. Zu diesem Zweck leitet StripedFly die Kommunikation durch einen eigens entwickelten TOR-Klienten. Kaspersky macht darauf aufmerksam, dass die Nutzung von EternalBlue durch StripedFly bereits 2016, über ein Jahr vor der Veröffentlichung des Exploits durch die Shadow Brokers-Gruppe am 14. April 2017, beobachtet wurde. Diesen Erkenntnissen zufolge experimentierte StripedFly mit der Tarnung von Spionageaktionen als Cryptominer bevor NotPetya im Juni 2017 versuchte, Sabotageabsichten hinter einem vordergründigen Ransomware-Angriff zu verbergen.

Der zweithäufigste im Oktober festgestellte Operationstyp war „Disruption“-Operationen (48%). 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 38 durch das Repositorium erfasst. Im Fall von Ransomware kann der blockierte Zugriff auf betriebswichtige Daten allerdings auch über einen längeren Zeitraum für Ausfälle sorgen.

Ende Oktober dokumentierte Microsoft mehrere Kampagnen, in denen sich das Verbrecherkollektiv Octo Tempest vermehrt auf den Einsatz von Verschlüsselungstrojanern konzentriert hat. Auch bekannt unter den Bezeichnungen 0ktapus, Scattered Spider, UNC3944, Starfraud, Scatter Swine, und Muddled Libra war die Gruppe vorher durch die Vermarktung von Zugängen an kriminelle Dritte zur weiteren Ausbeutung in Erscheinung getreten.

Die seit Mitte 2023 beobachteten Veränderungen im Aktivitätsprofil von Octo Tempest fallen zeitlich mit Absprachen mit der Ransomware-Gruppe BlackCat/ALPHV zusammen. In Folge dieser Vereinbarung hat Octo Tempest die angedrohte Veröffentlichung von gestohlenen Daten über BlackCats Leakseite kommuniziert und Schadsoftware der Gruppe vor allem gegen Ziele im Gastgewerbe, Einzelhandel, der fertigenden Industrie, dem Finanzwesen und der Glücksspiel- sowie Technologiebranche verwandt.

BlackCat profitiert von diesem Bündnis durch ausgefeilte Social-Engineering-Techniken, mit denen sich Octo Tempest als Mitarbeiter der IT-Abteilungen und Helpdesk-Teams seiner Ziele ausgibt, um Anmeldedaten von tatsächlichen Mitarbeitenden zu erhalten oder diese dazu zu bringen, Fernzugriffswerkzeuge zu installieren. In dieser Rolle nehmen Octo Tempest-Mitglieder ebenfalls verdeckt an Incident-Response-Besprechungen ihrer Opfer teil, in der vermuteten Absicht das eigene Vorgehen anzupassen, um der

Entdeckung zu entgehen und die Präsenz in den Netzwerken zu sichern.

In einer drastischen Eskalation dieser Social-Engineering-Taktik, hat die Gruppe in Einzelfällen versucht, Zugangsdaten auch durch die Androhung von physischer Gewalt gegen Mitarbeitende und ihre Angehörigen zu erlangen.

Die täuschende Authentizität dieser Anbahnungen, die Octo Tempest auszeichnet, geht mutmaßlich auf englische Muttersprachler in der Gruppe zurück. Sicherheitsanalysten schätzen, dass die Gruppe Mitglieder in Großbritannien und den USA umfasst. Vor dem Hintergrund dieser vermuteten Zusammensetzung von Octo Tempest erscheint die Zusammenarbeit mit der russischsprachigen Orientierung von BlackCat eine ungewöhnliche Konstellation. Operative Verbindungen dieser Art in die Jurisdiktionen der Opfer sind selten. Mitglieder, die beispielsweise von den USA aus agieren, bedeuten ein Risiko für Ransomware-Netzwerke, wenn diese Komplizen von dortigen Strafverfolgungsbehörden gefasst und interne Details über die Operationsweise bekannt werden.

Historisch betrachtet hat sich der Einsatz von BlackCat-Ransomware stark auf Organisationen in den USA konzentriert. Bei der überwiegenden Mehrheit der von BlackCat bis September 2022 identifizierten Opfer handelt es sich um US-amerikanische Ziele (58,7%). Es bestehen Anzeichen, dass BlackCat mit diesem Schwerpunkt beabsichtigt, die ab Mitte Dezember für öffentlich gehandelte Unternehmen greifenden Meldepflichten gegenüber der US-amerikanischen Börsenaufsicht als zusätzliches Druckmittel zu nutzen, um Lösegeldzahlungen zu forcieren.

Dieser operative Fußabdruck von BlackCat/ALPHV deckt sich mit der ausgeprägten geografischen Zielpräferenz von Scattered Spider auf in den USA-ansässige Organisationen.

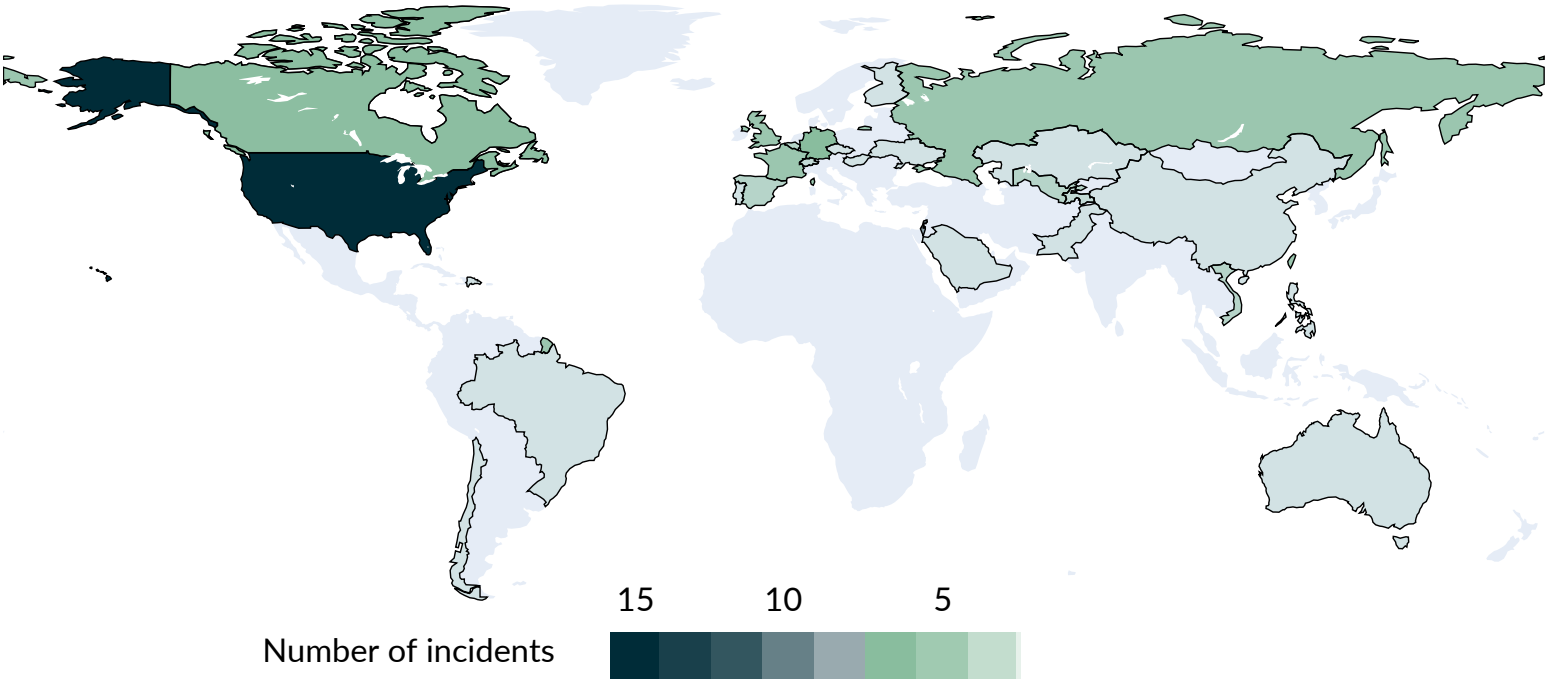
Sicherheitsanalysten nehmen an dass es sich bei der im November 2021 in Aktion getretenen Gruppierung BlackCat/ALPHV um eine Formation von ehemaligen Entwicklern aus dem Umfeld von Darkside handelt. Diese zwischenzeitlich aufgelöste Gruppe zeichnete sich unter anderem für den Ransomware-Angriff Colonial Pipeline verantwortlich, der im Mai 2021 in den USA für Unterbrechungen in der Treibstoffverteilung sorgte. Darkside stand im Verdacht Verbindungen zu REvil zu unterhalten. Mehrere Mitglieder von REvil wurden Anfang 2022 durch den FSB in Russland verhaftet. Das Weiße Haus geht davon aus, dass zumindest einer der Festgenommenen am Angriff auf Colonial Pipeline beteiligt war.

Um Aktivitäten von Octo Tempest aufzuklären und einen gemeinsamen Schutz aufzubauen, haben das FBI und CISA in einem Aufruf vom 16. November um Informationen über die Kommunikationsweisen und Verschlüsselungstechniken der Gruppe gebeten.

Brennpunkte und Zielmuster

Der am häufigsten im Oktober 2023 betroffene Zielsektor war, wie auch schon im Vormonat, Unternehmen der Kritischen Infrastruktur mit 39 Fällen beziehungsweise 49% der neu aufgenommenen Fälle. Dies ist ein Rückgang um ein Viertel zu den 50 Fällen im September, der sich auch auf relativer Ebene - in den Vormonaten hatten jeweils etwa drei von fünf aufgenommenen Vorfällen betroffene kritische Infrastrukturen - niederschlägt.

Geographic distribution of operations



Am zweithäufigsten betroffen waren in 34 Fällen (43%) staatliche Institutionen, was ebenfalls einen Rückgang darstellt, relativ aber in etwa den Vormonaten entspricht.

Wenig überraschend befindet sich Israel in diesem Monat auch bei Cyberkonflikten besonders im Blickpunkt: Während die USA aufgrund ihrer technologischen Dominanz im Cyberraum weiterhin mit 14 Vorfällen oder fast einem Fünftel der Vorfälle am häufigsten betroffen sind, ist Israel nach dem Angriff der Hamas vom 7. Oktober mehrfach Ziel von Hacktivisten geworden, mit acht von uns aufgenommenen Vorfällen und damit am zweithäufigsten weltweit betroffen. Zu den einzelnen Vorfällen und ihrer Einbettung in den seit Jahrzehnten schwelenden Konflikt finden sich im weiteren Verlauf nähere Ausführungen
In 16 von uns aufgenommenen Fällen, die Mitgliedsstaaten der EU betrafen, war Deutschland mit fünf Vorfällen der am häufigsten betroffene Mitgliedstaat und auch weltweit an dritter Stelle. Es folgten Großbritannien und Taiwan mit vier Vorfällen und - als nächster EU-Mitgliedstaat - Frankreich mit drei Vorfällen.

Von den Unternehmen der kritischen Infrastruktur betrafen die meisten Vorfälle solche im Telekommunikationssektor (neun Fälle). Darunter fanden sich disruptive Operation - teils in Verbindung zum Krieg in Nahost wie ein DDoS-Angriff auf brasilianische Internetdienstleister, teils ohne ersichtliche Verbindung hierzu ein Vorfall beim britischen Mobilfunkanbieter LycaMobile und zuletzt zwei Vorfälle (hier und hier) mit Bezug zum Krieg in der Ukraine. Mehrere Vorfälle stellen sich wiederum als “klassische” Ransomware von Cyberkriminellen dar und betrafen ein chilenisches Telekommunikationsunternehmen oder Südwestfalen-IT, einen IT-Dienstleister mehrere Dutzend Kommunen in Deutschland.

Ebenfalls häufig betroffen bleiben der Gesundheitssektor mit acht neu aufgenommenen Vorfällen und der Bereich “Critical Manufacturing” mit sechs Vorfällen. Für den Gesundheitsbereich sind die Mehrzahl der Angriffe disruptiver Natur, wobei die Intensität von mehreren DDoS-Angriffen auf Webseiten von Klinken in Israel (dazu sogleich) und Kanada bis hin zu

Betriebsstörungen in einer schweizerischen Psychiatrie oder bei zwei Krankenhäusern in Frankreich reicht. In vergleichbaren Vorfällen in der Vergangenheit war hier der Einsatz von Ransomware häufig mitursächlich, der nach Angaben von ENISA die größte Gefahr für den Gesundheitssektor darstellt. In den konkreten Fällen dieses Monats wurde der Einsatz von Ransomware nicht öffentlich bekannt.

Für den Bereich Critical Manufacturing lässt sich zusammenfassend erkennen, dass der Diebstahl von vertraulichen Daten im Vordergrund steht. Auch hier kann es sich zunächst "nur" um den Versuch von Cyberkriminellen handeln, mit Hilfe von gestohlenen Daten Lösegeldzahlungen zu erpressen, wie es sich in Fällen der Gruppe Octo Tempest oder bei der US-amerikanischen BHI Energy zeigt. Weiterhin sind aber auch Fälle mit dem Ziel der Industriespionage in diesem Bereich üblich und sind für Oktober etwa für mehrere Unternehmen im Verteidigungsbereich oder asiatische Unternehmen der Halbleiterindustrie bekannt geworden.

Bei den betroffenen staatlichen Institutionen waren in der Hälfte der Fälle Regierungsbehörden und andere Institutionen auf nationaler Ebene betroffen, während für den Bereich "Civil Service/Administration", in dem Angriffe auf nachrangige Behörden erfasst werden, 14 neue Vorfälle oder 41% aller staatlichen Institutionen aufgenommen wurden. Das in den letzten Monaten wahrgenommene "Muster" der zunehmenden Schwere von Cybervorfällen subnationalen öffentlichen Institutionen ebenso wie in Staaten mit einem niedrigeren Cybersicherheitsniveau lässt sich auf für den Oktober wiedererkennen: Cybervorfälle, die Regierungsbehörden etwa in Australien, Belgien (hier und hier) und Tschechien betrafen, fallen allesamt in die Kategorie "DDoS-Angriffe". Von schwererwiegenden Datendiebstählen mit oder ohne dem Einsatz von Ransomware waren demgegenüber mit Guyana, der Mongolei und Staaten in Zentralasien Länder außerhalb Europas und Nordamerikas, deren Cyberverteidigung als schwächer wahrgenommen wird. Gleiches gilt für öffentliche Einrichtungen auf der subnationalen Ebene und betrafen in Deutschland etwa Hochschule Hannover sowie die Kommune Grasellenbach. Der letzte Angriff mit deutschen Betroffenen waren DDoS-Angriffe auf die Webseiten mehrerer Kommunen Mitte des Monats.

Angreiferprofile und Attributionen

Auch im Oktober konnte ein Großteil der erfassten Cyberoperationen (bislang) keinem Verantwortlichem zugesprochen werden, so blieb in 67 Prozent der Fälle (54) die Urheberschaft noch unklar, was der Prozentzahl des Vormonats September entspricht. In 28 der 79 Fälle wurden nicht staatliche Akteure verantwortlich gemacht, was prozentual einen Anstieg von ca. 4% im Vergleich zum Vormonat September bedeutet. Von diesen 28 Fällen wurden 16 ideologisch/politisch motivierten Hacktivisten und 12 finanziell motivierten Cyberkriminellen angelastet, bzw. zumeist von diesen Akteuren entsprechend für sich reklamiert.

Auf dem ersten Platz der attribuierten Angreifer(herkunfts)länder stehen mit jeweils 5 erfassten Cyberoperationen Russland, Nordkorea und die Ukraine, was auch zu einer wieder deutlich erhöhten Anzahl an Vorfällen im Rahmen des

russischen Krieges gegen die Ukraine führte (10), im Vergleich zum September (3). China und Iran rangieren entsprechend des übergeordneten Trends der letzten Monate auch im Oktober ebenfalls wieder unter den Top-Angreiferländern.

Im Oktober schafften es jedoch zudem gleich zwei “Newcomer” in die Liste, die seit April bisher dort nicht erschienen sind: Kasachstan und Jordanien. Die erfassten Fälle sind jedoch höchst unterschiedlich gelagert: Für das erstgenannte Land wurde seitens der Threat Intelligence Abteilung von Cisco Talos eine Cyberspionage-Operation der APT YoroTrooper öffentlich gemacht, die kritische Infrastrukturen und staatliche Ziele der Gemeinschaft unabhängiger Staaten (GUS) seit Juni 2023 mit Spearphishing anvisierte. Auch wenn keine direkte Verbindung zu staatlichen Stellen behauptet wurde, wäre dies durchaus plausibel, zumal YoroTrooper im Rahmen einer False-Flag Operation versuchte, den Verdacht auf Aserbaidschan als Ursprungsland der Spionage zu lenken. Dagegen handelte es sich bei der Hack-and-Leak Operation jordanischer Hacktivisten gegen das israelische Ono Academic College vom 9. Oktober und damit zwei Tage nach den Gewalttaten der Hamas gegen Israel um eine “klassische” Hacktivisten-Operation im Kontext eines gewaltsamen Konfliktes, der vor allem im Cyberspace eben auch schnell eine transnationale Komponente entwickelt. Dies stellt somit eine Parallele zu den beobachteten Hacktivisten-Vorfällen im Rahmen des russischen Krieges gegen die Ukraine dar: auch hier solidarisierten sich im Zuge der Invasion vom 24. Februar 2022 schnell bereits existierende Hacktivisten-Gruppierungen mit der einen oder anderen Seite oder formierten sich gar erst neu aufgrund der geopolitischen Ereignisse. Für den Konflikt zwischen Israel und der Hamas wurden in der EuRepoC-Datenbank im Oktober 2023 elf Vorfälle erfasst, somit sogar noch einer mehr als für den Ukraine-Russland Krieg. Da EuRepoC lediglich solche Fälle in die Datenbank aufnimmt, die einen beobachtbaren Schaden angerichtet haben (Verletzung der “CIA-Triade der Informationssicherheit”) und zudem nicht nur ausschließlich vom Angreifer selbst berichtet, sondern noch von weiteren, unabhängigen Quellen thematisiert wurden, liegt diese Zahl deutlich niedriger als in vielen Medienberichten zur Cyberkomponente der Auseinandersetzungen in Nahost, die in Teilen ungeprüft die Behauptungen von Angreifern übernehmen.

Ein Beispiel einer solchen Falschbehauptung war der angebliche Hack des privaten Dorad Kraftwerks in Aschkelon am 8. Oktober, somit nur einen Tag nach der Eskalation der Hamas. Die pro-iranische Gruppe Cyber Av3ngers hatte einen umfangreichen DDoS-Angriff auf die kritische Infrastruktur via Social Media für sich reklamiert und hierfür auch angebliche Beweise in Form von Screenshots präsentiert. Diese stellten sich jedoch relativ schnell als Fotos eines bereits vergangenen Hacks der ebenfalls pro-iranischen Gruppierung Moses Staff gegen ein israelisches Ziel aus 2022 heraus. Gerade politisch-motivierte Hacktivisten-Vorfälle fanden somit nicht immer zwangsläufig auch in der behaupteten Form statt, oder aber verursachten nicht unbedingt die von den Tätern angegebenen Schäden, oder aber waren eigentlich das Werk einer anderen Gruppe.

Nichtsdestotrotz stieg das Cyberoperationsniveau im Kontext des Konfliktes seit dem 7. Oktober erheblich an, was sich auch in den Daten des Repositorys widerspiegelt. In acht der 11 dem Konflikt zugeordneten Cybervorfälle waren israelische Ziele betroffen, in zweien (pro-)palästinensische und in einem mit Brasilien eine Drittpartei. Auch dies ist eine Parallele zu den erfassten Cybervorfällen im Rahmen des russischen Krieges gegen die Ukraine: die Mehrzahl der Hacks richten sich gegen das angegriffene Land, ein weiterer Teil jedoch auch gegen Ziele der ursprünglich angreifenden Partei sowie gegen Staaten/Akteure, die erstere unterstützen. Brasilien stellte hierfür jedoch genau genommen nicht das am ehesten zu erwartende Zielland anti-israelischer/pro-palästinensischer Hacker dar. Zwar hatte Brasilien am 18. Oktober einen Resolutionsentwurf in der UN eingebracht, in der u.a. die Gewalt der Hamas verurteilt wurde, jedoch übt die Regierung gleichzeitig Druck auf Israel auf, die Entlassung der in der Gewalt der Hamas befindlichen, u.a. auch brasilianischen Geiseln, stärker zu forcieren, u.a. auch durch Feuerpausen. Der Vorfall könnte somit auch Ausdruck einer in Teilen opportunistischen Zielauswahl-Logik mancher Hacktivisten-Gruppierungen sein, bei der eher die (zeitnahe) Verwundbarkeit eines Opfers aus technischer Sicht eine Rolle für deren Anvisieren spielt.

In jedem Falle könnten Cyberoperationen gegen israelische, sowie das Land unterstützende Staaten weiter zu nehmen. Von Bedeutung für die Intensität und Schwere dieser Fälle wird zudem sein, inwiefern sich iranische APTs auf die Seite der Hamas im Cyberspace schlagen. Analysten von Microsoft hatten auf einer Cybersicherheitskonferenz Anfang November berichtet, dass sie keine Anhaltspunkte gefunden hätten, dass iranische APTs auf den Angriff der Hamas vorbereitet, d.h. darüber im Vorfeld informiert gewesen wären. Dennoch passten diese in Teilen ihre bereits laufenden Operationen nach dem 7. Oktober entsprechend an, um die Hamas in der Folge zu unterstützen, laut Microsoft jedoch erst ab dem 18. Oktober. Auch wenn die Konstellation im Falle Russlands eine andere war und ist, da das Land im Gegensatz zur Hamas im Cyberspace wesentlich autonomer agieren und weniger auf einen “Cyber-Patron” angewiesen ist, verdeutlichen die bisherigen Cyberkonflikt-Dynamiken im Kontext des Konfliktes zwischen Israel und der Hamas wie im Falle der Ukraine auch, dass tatsächlich kriegsentscheidende Konfliktaustragungsmittel nach wie vor eher auf der konventionell-militärischen Ebene angesiedelt sind und Cyberoperationen allenfalls eine unterstützende Rolle spielen. Ebenfalls wie im Falle der Ukraine zeigen jedoch auch Beispiele von pro-Hamas

Hacks, etwa gegen israelische Werbetafeln, dass Cyberoperationen in gewaltsamen Konflikten vor allem auch auf die psychologische Zersetzung und Beeinflussung der gegnerischen Bevölkerung ausgerichtet sein können, um diese in Angst und Schrecken zu versetzen und ihre Kampfmoral somit potenziell zu schwächen. Zuletzt könnten DDoS-Operationen der mutmaßlich russischen False-Flag Gruppe Anonymous Sudan gegen israelische Ziele vom 7. Oktober andeuten, dass sich die Hacktivisten-Sphären der beiden aktuell gewaltsamsten geopolitischen Konflikte in Zukunft miteinander vermischen könnten, was die Herausforderung der Attribution von Motivationen und Verantwortlichkeiten weiter erschweren könnte.
Eine weitere Konfliktdyade des Nahen Ostens, die ebenfalls Auswirkungen auf den Fortgang des Krieges zwischen der Hamas und Israel haben könnte, ist Iran vs. Saudi-Arabien. Denn auch wenn im März 2023 unter der Vermittlung der Volksrepublik China und unter Ausschluss der USA eine Art Friedensabkommen zwischen den historisch verfeindeten Staaten geschlossen wurde, zeigt ein im Oktober bekannt gewordener iranischer Cyberspionageakt gegen saudische Ziele ab August 2023, dass angebliche Entspannungen zwischen Staaten nicht gleichbedeutend mit einem Stopp jeglicher Cyberkonfliktaktivitäten sind. Darüber hinaus wird politisch motivierte Spionage allgemein als nicht-völkerrechtswidrig angesehen und wird daher - insofern sie etwa nicht zur direkten Vorbereitung disruptiver Operationen dient, oder nicht den Auftakt einer kompromittierenden Hack-and-Leak Operation darstellt -, auch in den selteneren Fällen zu einer Eskalation einer Konfliktdyade führen. Stattdessen können Cyberspionageoperationen Staaten potenziell auch dazu dienen, um sich von der (Nicht-)Einhaltung der in zwischenstaatlichen Vereinbarungen festgeschriebenen Verpflichtungen seitens des politischen Gegenübers zu überzeugen.

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 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).