European
Repository of
Cyber Incidents

EuRepoC

Cyber Conflict Briefing

Q3 2025

Jakob Bund
Lena Rottinger
Kerstin Zettl-Schabath

Beobachtungen zur Gesamtlage

Im **Q3 2025** wurden 224 Cyber-Operationen in die EuRepoC-Datenbank aufgenommen. Das sind 24,4% mehr als im vorausgehenden Quartal und 38 Operationen mehr als die insgesamt durchschnittlich verzeichnete Aktivität von 186 Cyber-Operationen pro Quartal im Gesamtzeitraum.

Die **durchschnittliche Intensität** der in Q3 2025 erfassten Operationen beträgt 3,24 und liegt somit über dem historischen Durchschnitt (2,88). 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

Das Cyber Conflict Briefing analysiert Entwicklungen in der Bedrohungslandschaft auf Grundlage der von **EuRepoC** erfassten Cybervorfällen. Für diese Auswertung stehen technische, politische sowie rechtliche Aspekte im Vordergrund. Seit Oktober 2025 veröffentlicht EuRepoC das Briefing quartalsweise in Zusammenarbeit mit der **Deutschen Cyber-Sicherheitsorganisation GmbH (DCSO)**.

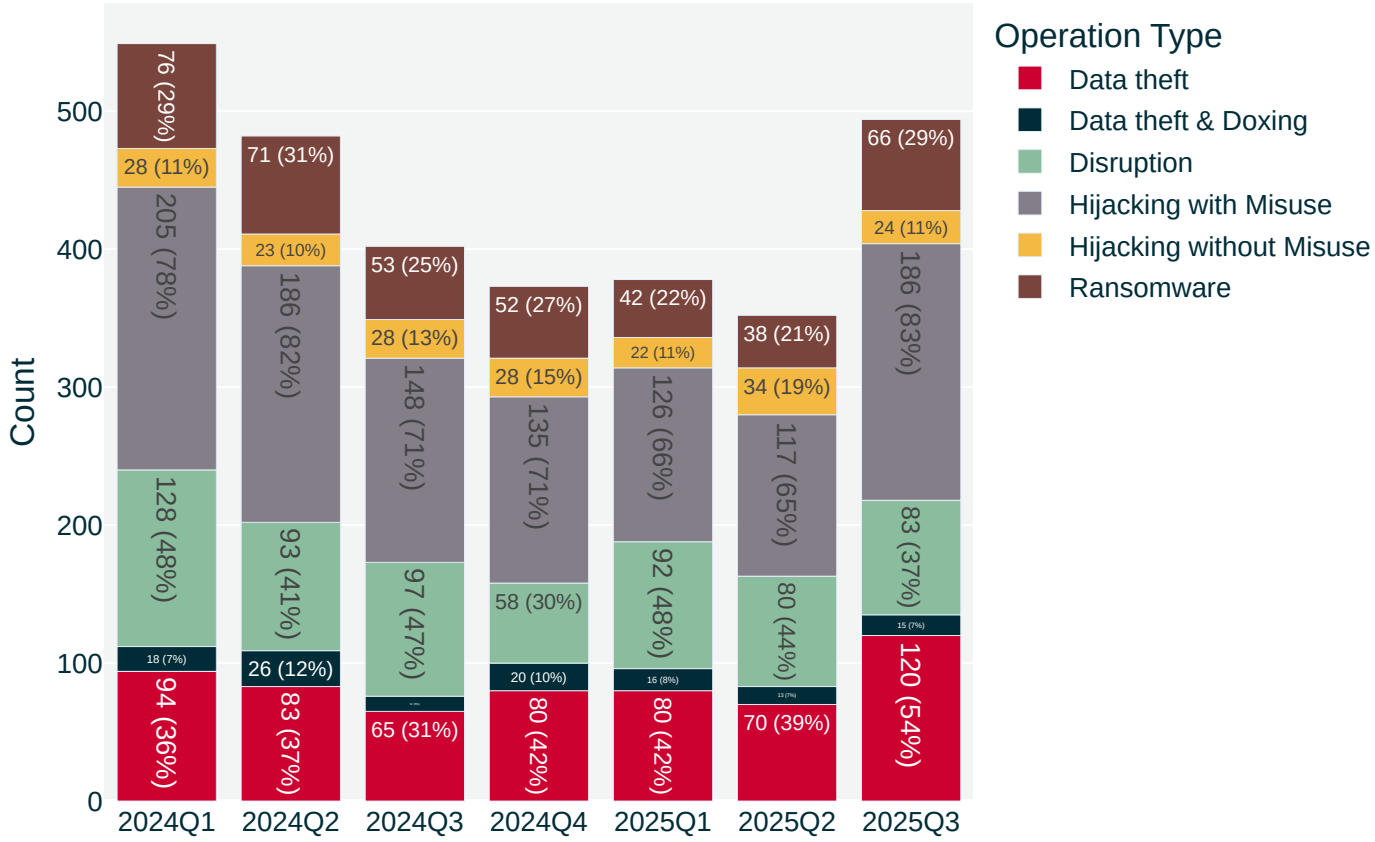
Die deutsche Ausgabe erscheint in Kooperation mit dem **Tagesspiegel Cybersecurity Background.**

European
Repository of
Cyber Incidents

DCSO

Die im Q3 2025 erfassten Vorfälle verteilen sich auf folgende **Operationstypen**:

Verteilung der in Q3 2025 beobachteten Aktivitäten nach Operationstyp



Hinweis: Einzelne Cybervorfälle können mehrere Operationstypen in Kombination aufweisen.

Insider-Bedrohungen breiten sich mit KI-Unterstützung aus

Der größte Anteil umfasst 'Hijacking with Misuse' - Operationen mit 186 Fällen (83%). In diesem Zusammenhang fallen vermehrt Bemühungen nordkoreanischer IT-Fachkräfte auf, sich verdeckt in Organisationen einzuschleusen. Durch Social Engineering-Techniken versuchen diese Gruppen ihre tatsächliche Identität zu verschleiern, um in regulären Bewerbungsverfahren der betroffenen Firmen zu bestehen und im Fall einer Einstellung direkten Zugriff auf interne Systeme über legitime Zugänge zu gewinnen.

Im Unterschied zum Social Engineering-Einsatz wie er sich üblicherweise für kriminelle Akteure beobachten lässt, zielen diese nordkoreanischen Aktivitäten zunächst darauf ab, über solche Beschäftigungen Einkünfte zu generieren. Entsprechend längerfristig sind sie in die Aufrechterhaltung der vorgegebenen Identität investiert und erfüllen in dieser Rolle zugewiesene Arbeitsaufträge vielfach verlässlich und zur Zufriedenheit der Arbeitgeber. Parallel dazu nutzen diese Gruppen ihre internen Zugänge, um weitere Monetarisierungsmöglichkeiten auszuspähen.

Im Unterschied zum Social Engineering-Einsatz wie er sich üblicherweise für kriminelle Akteure beobachten lässt, zielen diese nordkoreanischen Aktivitäten zunächst darauf ab, über solche Beschäftigungen Einkünfte zu generieren. Entsprechend längerfristig sind sie in die Aufrechterhaltung der vorgegebenen Identität investiert und erfüllen in dieser Rolle zugewiesene Arbeitsaufträge vielfach verlässlich und zur Zufriedenheit der Arbeitgeber. Parallel dazu nutzen diese Gruppen ihre internen Zugänge, um weitere Monetarisierungsmöglichkeiten auszuspähen.

Insbesondere Firmen im Kryptowährungsbereich oder mit Kryptowährungsbeständen stellen attraktive Ziele dar. Aber auch ein breiteres Segment von Unternehmen ist anfällig für Ransomware oder Datendiebstahl, wenn Bedrohungsakteure ihre Entdeckung befürchten und in einem Exit-Scam versuchen, ihren finanziellen Gewinn zu maximieren bevor sie ihren Zugang verlieren.

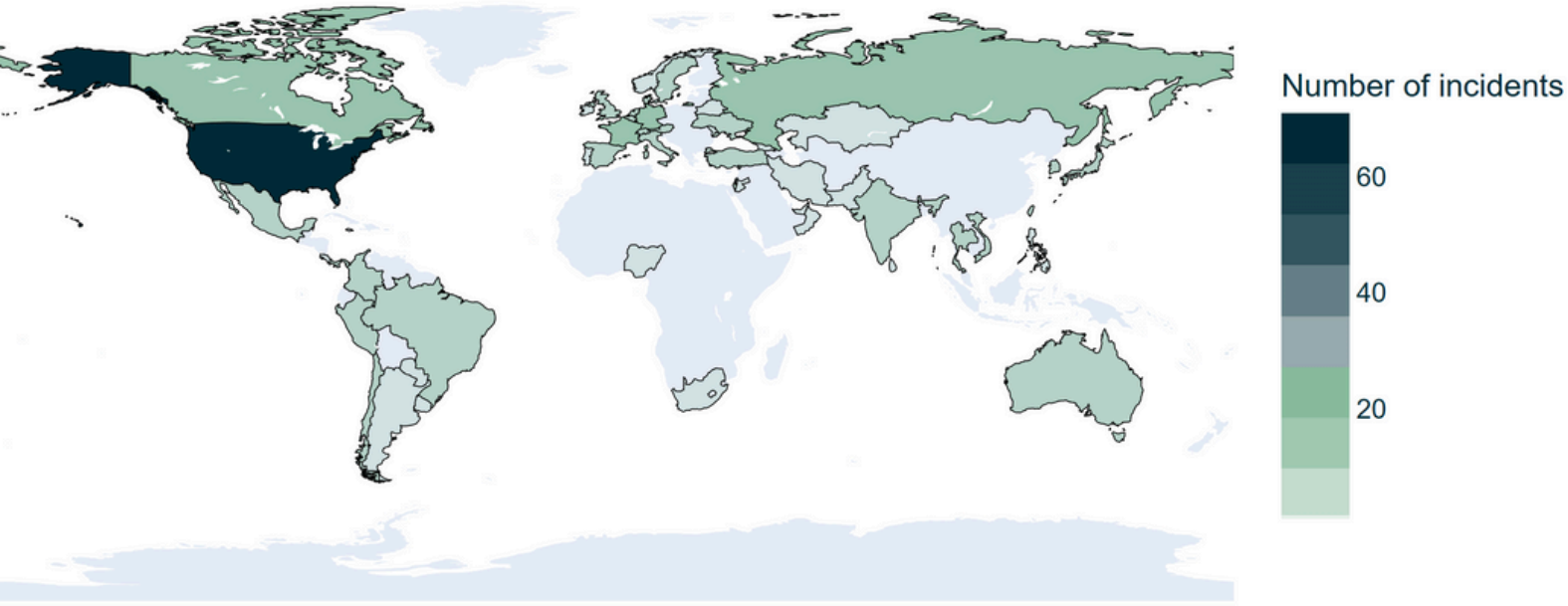
Beispielhaft beobachten ließen sich diese Entwicklungen im dritten Quartal 2025 für mehrere NFT-Projekte, die unter anderem auf die Ausstellung digitaler Zertifikate für den fälschungssicheren Handel von virtueller Kunst spezialisiert sind. Neben dem Marktplatz Favrr wurden die Projekte Replicandy und ChainSaw Ende Juni Opfer einer solchen Kampagne.

Diese Projekte hatten zuvor unwissentlich nordkoreanische Programmierer als Software-Entwickler und, im Fall von Favrr, als Chief Technology Officer eingestellt. Diesen Akteuren gelang es, massenhaft Zertifikate auszufertigen und durch den blitzartigen Verkauf digitaler Assets Beträge in Höhe von knapp einer Million Euro abzuschöpfen.

Unter der Zuhilfenahme von KI-Werkzeuge ist ein wachsender Pool an nordkoreanischen IT-Kräften in der Lage, in solche Einflusspositionen zu gelangen. Anthropic, der Entwickler hinter dem Large Language Model und dem darauf basierenden Chatbot Claude, beobachtet den Einsatz des eigenen Tools verstärkt durch Akteure, die anderweitig weder über die notwendigen Sprach- noch Technikkenntnisse verfügen, um Einstellungsverfahren erfolgreich zu durchlaufen oder die danach im Betriebsalltag an sie gestellten Arbeitsanforderungen zu erfüllen. Die so abgesenkte Einstiegshürde befähigt nicht nur eine größere Zahl an Angreifern, sondern schafft Kapazitäten für diese Akteure, ihre Aktivitäten über den bisherigen Zielbereich gut bezahlender Technologieunternehmen hinaus auf kleinere und mittelständische Firmen auszudehnen.

Diese Verschiebung hin zu niedrigschwelligeren Zielen zeichnet sich im Fall der im Juni betroffenen NFT-Projekte ab. Dabei verfügen gerade kleinere Unternehmen häufig nur über eingeschränkte Fähigkeiten, um diese Insider-Bedrohungen zu entdecken.

Geografische Verteilung der betroffenen Organisationen Q3 2025



Spionagebedrohungen passen sich an geopolitische Prioritäten an

Der zweithäufigste in Q3 festgestellte Operationstyp war 'Data theft'-Operationen (54%). Von diesen Operationstypen sind 120 Fälle durch das Repository erfasst. Gleich mehrere lang andauernde Spionagekampagnen mit vermuteter Verbindung nach China sind in diesem Zeitraum dokumentiert. Der Zugriff erfolgt häufig über Schwachstellen in schwer zu überwachenden Netzwerkgeräten, wie Firewalls oder VPN-Appliances.
Neben den im weiteren Verlauf beschriebenen Aktivitäten des Salt Typhoon-Clusters sind insbesondere Versuche der Gruppierung UNC5221, über lange Zeit unentdeckt Ziele aufzuklären, auffällig. Dabei nutzt UNC5221 auch zuvor unbekannte Sicherheitslücken, um Netzwerkequipment zu kompromittieren und durch das Einrichten von Backdoors langfristig den Zugang zu sichern. Die lange Aufenthaltszeit in Netzwerken erschwert zudem regelmäßig Aufklärungsbemühungen. In Incident-Response-Einsätzen beobachtete etwa die Cybersicherheitsfirma Mandiant eine durchschnittliche Verweildauer von 393 Tagen für die Bedrohungsakteure.
In vielen Fällen übersteigt diese Spanne die Aufbewahrungsdauer für Logs und behindert damit eine weitere Zurückverfolgung der Aktivitäten.
In den im September bekannt gewordenen Fällen konzentrierte sich UNC5221 zuletzt auf juristische Dienstleister sowie Technologieunternehmen, Software-as-a-Service-Anbieter und andere externe Dienstleister für das Outsourcen von Geschäftsprozessen. Wie Mandiant berichtet geht das Interesse an diesen Organisationen über Spionageinteresse hinaus. Solche Zugänge zu Dienstleistern und IT-Herstellern können als Brückenköpfe dienen, um in Folge Kundenunternehmen oder Informationen zur weiteren Schwachstellenentwicklung zu erreichen.
Die mutmaßlich von handelspolitischen Interessen angeleiteten Ausspähversuche gegen juristische Dienstleister verdeutlichen daneben den strategischen Wert der Backdoors und den damit verbundenen dauerhaften Zugriffsmöglichkeiten. Über diese Kanäle können Bedrohungsakteure agil auf sich verändernde Informationsbedürfnisse reagieren und an geopolitische Entwicklungen anpassen.

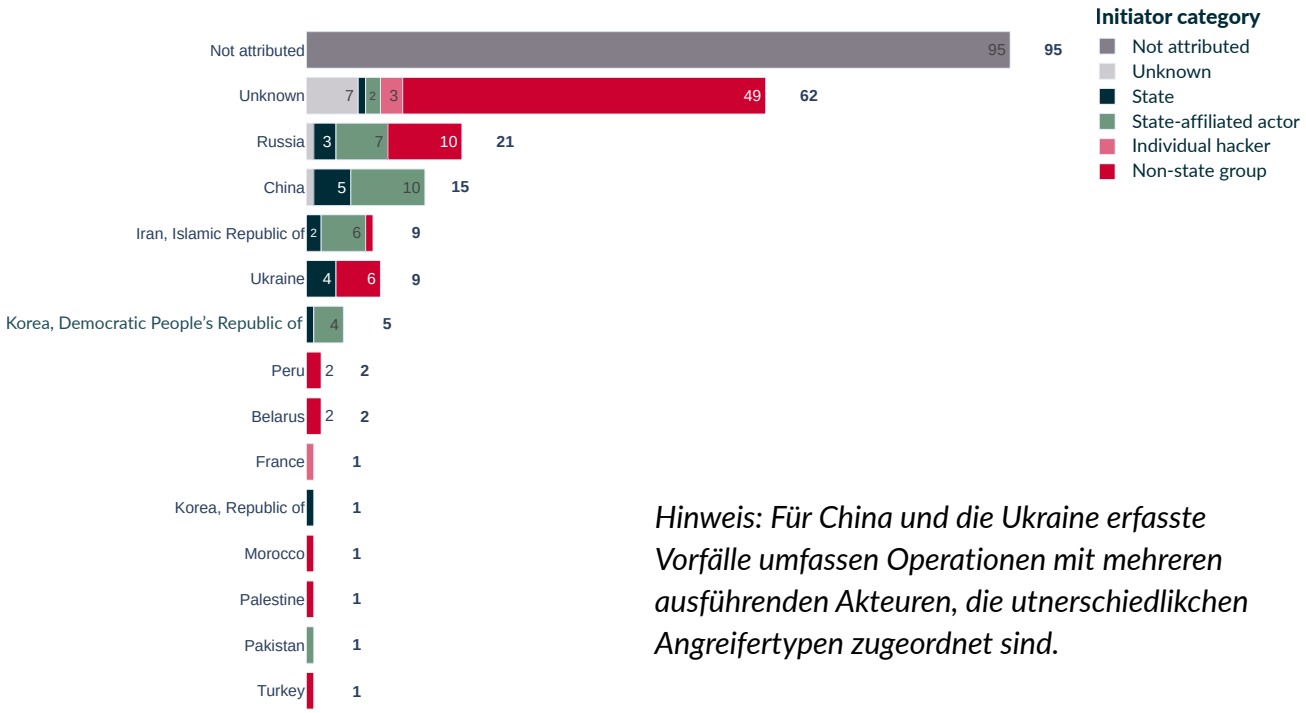
Angreiferprofile und Attributionen

Im dritten Quartal wurden 42% der Cybervorfälle nicht oder noch nicht attribuiert. Die Kategorie „Unbekannt“ (nur 4% der Fälle) gibt Auskunft über den Anteil der dokumentierten Vorfälle, bei denen zwar der Angreifertyp, aber nicht das Ursprungsland bekannt ist. Von den bekannten Angreifertypen waren nicht-staatliche Hackergruppen mit 75 Operationen (33%) am aktivsten. Dem genannten Typus lassen sich Cyberkriminelle, darunter Ransomware-Gruppierungen wie Scattered Spider, ebenso zuordnen wie Hacktivisten, z.B. die prorussischen Gruppe NoName057(16). 13% der Vorfälle gingen von Akteuren aus, die entweder staatlich unterstützt oder bei den eine Verbindung zu einem nationalstaatlichen Akteur vermutet wird. Bei 17 Vorfällen war gab es eine klare Attribution zu einem staatlichen Akteur, wobei fünf dieser Vorfälle der Volksrepublik China zugeordnet wurden.

Für die im dritten Quartal hinzugefügten Cyberoperationen zeigen sich neben beständig aktiven Bedrohungsakteuren aus China, Russland, Iran und Nordkorea, auch Frankreich, Malaysia, Südkorea, Marokko, Peru, Belarus, die Türkei, Palästina und die Ukraine als Ursprungsländer. Besonders viel Aktivität dokumentierte EuRepoC – ähnlich wie in den Vormonaten – im Rahmen Russlands fortlaufender Aggression gegen die Ukraine zwischen diesen beiden Ländern. Erstmalig identifizierte das ukrainische CERT eine neue russische Malware namens LameHug, die ein KI-gestütztes großes Sprachmodell (LLM) nutzt, um Befehle zur Ausführung auf kompromittierten Windows-Systemen zu generieren. CERT-UA attribuierte diesen Vorfall mit „mäßiger Sicherheit“ zu APT28, einer Gruppe, die mutmaßlich aus dem russischen Militärgeheimdienst GRU heraus operiert.

Abgesehen von Russlands Aktivitäten in der Ukraine sind auch weitere russische Cyberoperationen gegen politische Ziele bekannt geworden, darunter eine dem FSB zugeordnete Spionagekampagne der Turla-Gruppe gegen ausländische Botschaften in Moskau und der Angriff auf die zentrale Wahlkommission in Moldau kurz vor der entscheidenden Parlamentswahl Ende September. Auch Justizbehörden in den USA und den Niederlanden waren im Visier russischer Angreifer, die sich Zugang zu sensiblen und teilweise versiegelten Gerichtsdokumenten verschaffen konnten. Besonders heikel ist das im Fall der USA, da die Angreifer Zugriff auf Informationen über Zeugen und Quellen laufender Gerichtsprozesse und Personen erlangten, denen Verbrechen gegen die nationale Sicherheit vorgeworfen wird. Während US-Senator Ron Wyden in einem öffentlichen Brief seine Besorgnis über die Sicherheit der US-amerikanischen Justizsysteme zum Ausdruck brachte, normalisierte US-Präsident Donald Trump die Aktivitäten als eine Fortschreibung russischer Verhaltensweisen. Die ständige Konfrontation mit Hackerangriffen folge einem bekannten Muster. Gleichzeitig betonte Trump, dass die Fähigkeiten der USA den russischen überlegen seien. Mit Blick auf den kurze Zeit später stattfindenden USA-Russland-Gipfel zog Präsident Trump in Erwägung, den Vorfall mit Russlands Präsident Vladimir Putin zu diskutieren.

Suspected geographic origin of initiators Q3 2025



Hinweis: Für China und die Ukraine erfasste Vorfälle umfassen Operationen mit mehreren ausführenden Akteuren, die utnerschiedlikchen Angreifertypen zugeordnet sind.

Koordiniertes Vorgehen gegen Spionagebedrohungen aus China

Besonders auffällig im dritten Quartal waren neben den russischen Operationen die Hackeraktivitäten von chinesischen Bedrohungsakteuren. In diesem Kontext standen vor allem staatlich geförderte Aktivitäten, die öffentlich unter dem Namen Salt Typhoon verfolgt werden, im Fokus der westlichen Geheimdienste und Medien. Salt Typhoon-Akteure hatten sich im März 2024 Zugang zum Netzwerk der US Army National Guard verschafft und blieben dort für neun Monate unentdeckt. Erst im Juli 2025 gelangte dieser Vorfall durch den Leak eines internen Memos des Department of Homeland Security an die Öffentlichkeit und wurde damit in der EuRepoC Datenbank hinzugefügt. Durch die Kompromittierung des Netzwerks gelangten die Angreifer an Daten, mit denen China prinzipiell auch Zugang zu weiteren US Army National Guard-Einheiten erlangen könnte. Dieser Vorfall reihte sich in eine lange weiterer bekannter Ziele Salt Typhoons ein, zu denen vor allem Regierungsinstitutionen und kritische Infrastrukturbetreiber wie Telekommunikationsunternehmen zählen. Beispielsweise kompromittierte derselbe Akteur bereits AT&T, Lumen, Verizon, Windstream, Charter und Viasat.
Das erhebliche Ausmaß der Spionageaktivitäten mit Verbindung zu Salt Typhoon wurde zusätzlich am 27. August 2025 mit einem Joint Advisory der IT-Sicherheitsbehörden und Nachrichtendienste von zehn Staaten, darunter USA; Großbritannien und Deutschland, unterstrichen. In dem Dokument warnen die Behörden vor einer weit zurückreichenden globalen Kampagne. Akteure aus dem Salt Typhoon-Cluster sind nach diesen Einschätzungen seit mindestens 2021 aktiv. Entsprechende Aktivitäten oder sich zumindest in Teilen überschneidende Beobachtungen sind auch unter den Namen OPERATOR PANDA, RedMike, UNC5807, und GhostEmperor dokumentiert. Die am Joint Advisory beteiligten Nachrichtendienste konnten dabei eine Verbindung zwischen Salt Typhoon-Operationen und drei in China ansässigen Unternehmen herstellen, die Produkte und Dienstleistungen für Chinas Ministerium für Staatssicherheit und mehrere Einheiten der Volksbefreiungsarmee bereitstellen.

Die New York Times bewertete dieses Vorgehen als eine „äußerst ungewöhnliche gemeinsame Erklärung“, da die Anzahl der unterzeichnenden Staaten verhältnismäßig hoch ist und sich sonst eher zurückhaltende Staaten wie Italien und Spanien an dieser gemeinsamen „Naming-and-Shaming“-Strategie beteiligten. Cynthia Kaiser, ehemalige Beamtin des FBI und Leiterin der Ermittlungen, gehe nicht davon aus, dass irgendein US-Amerikaner oder irgendeine US-Amerikanerin von dieser Salt Typhoon-Spionageaktivität verschont geblieben sei. Zuletzt sei dabei aber nicht klar gewesen, ob es sich bei dieser Spionagetätigkeit um gezielte Abhörversuche oder den massenhaften Datendiebstahl zur weiteren Mustererkennung handelte.

Am 28. August 2025, am Tag nach der Publikation des Joint Advisory, veröffentlichte auch das niederländische Verteidigungsministerium eine Attribution, die vor einer „wachsenden chinesischen Cyberbedrohung“ warnt, auch wenn niederländische Organisationen nicht so stark betroffen seien, wie US-amerikanische. Ähnlich wie in der gemeinsamen Erklärung, beschreibt die niederländische Attribution, dass Salt Typhoon vor allem das Ziel hatte, Zugriff auf Router von Telekommunikationsunternehmen zu erlangen. Abgesehen von dieser politischen Attribution der Niederlande und der Beteiligung mehrerer europäischer Behörden im Joint Advisory blieb diese weitreichende chinesische Spionageaktivität (bisher) politisch ohne weitere Konsequenzen. Ein Sprecher des chinesischen Außenministeriums wies die Vorwürfe zurück und beschuldigte im Gegenzug die USA, das größte „Hacking-Imperium“ der Welt zu betreiben.

Schlagabtausch zwischen Cyberkriminellen und Strafverfolungsbehörden

Auch in den vergangenen drei Monaten hielt der Trend einer zunehmenden Zersplitterung des Cybercrime-Ökosystems an. Das anhaltende „Tit-for-Tat“ zwischen Ransomware-Gruppen und Strafverfolgungsbehörden prägte dabei das Geschehen. Mit wachsendem Ermittlungsdruck reagierten viele Akteure durch „Rebrandings“, wie die Transition von BackSuit zum neuen Namen „Chaos“ zeigt, und (zumeist) kurzlebige Neugründungen. Längerfristig bestehen dagegen häufig nur große, gut vernetzte Gruppen. Dass gerade diese sich des zunehmenden Drucks bewusst sind, zeigt u.a. das öffentlich gemachte Bestreben von DragonForce, mit anderen prägenden Ransomware-Gangs der letzten Monate, wie Qilin und Lockbit (5.0), eine Art Ransomware-Kartell gründen zu wollen.

Die Vorteile lägen auf der Hand: weniger Reibungsverluste durch Konkurrenz, effizientere Ressourcenteilung sowie erwartbarere Gewinne. Gleichzeitig würde dies im Falle eines tatsächlichen Zustandekommens eine Art Gegenpol (und vermutlich auch Reaktion) zur gegenläufigen Entwicklung des zunehmend gegenseitigen „Naming and Shamings“ bilden: Auch zwischen Juli und September beschuldigten Gruppierungen oder sog. „Affiliates“ andere Gangs (konkret die Qilin-Gruppe) sogenannter „Exit Scams“, oder einer Infiltrierung durch Strafverfolgungsbehörden, was das erschütterte Grundvertrauen innerhalb der Szene verdeutlicht.
Parallel dazu intensivierte sich die Verbindung zwischen Infostealer- und Ransomware-Strukturen.

Besonders das Lumma-Stealer-Ökosystem erwies sich als widerstandsfähig gegenüber Abschaltungen und bleibt ein fester Bestandteil moderner Angriffsketten. Diese technische Resilienz zeigt, dass sich Kriminelle zunehmend auf modulare und austauschbare Werkzeuge stützen, um Ermittlungsmaßnahmen zu umgehen.
Zugleich rückt eine neue Tätergeneration in den Fokus der Behörden. Immer häufiger geraten inländische, vor allem jugendliche Akteure in Europa in den Blick. Fälle wie die der Allianz zwischen LAPSUS$, ShinyHunters und Scattered Spider oder die Insider-„Angriffe“ britischer Schüler auf Schulen verdeutlichen, dass junge Täter inzwischen einen relevanten Anteil der Szene ausmachen, sei es als eigenständige Angreifer, als Teil organisierter Gruppen oder als leicht ersetzbare sogenannte „disposable agents“. Ihre geringere Mobilität erleichtert den Strafverfolgungsbehörden das Vorgehen, während auch technisch wenig versierte Personen zentrale Rollen innerhalb krimineller Kollektive wie Scattered Spider übernehmen können.

Gleichzeitig verschwimmen die politischen und geografischen Grenzen im Ransomware-Milieu zunehmend. Kooperationen zwischen Gruppen aus autoritären Staaten – etwa bei Pay2Key oder in Fällen russischer und chinesischer Beteiligung an nordkoreanischen „IT-Worker“-Betrugsfällen – deuten auf neue Arbeitsteilungen hin. Gleichzeitig kündigte LockBit mit LockBit 5.0 ihr neues Affiliate-Programm an, in dem Angriffe gegen besonders kritische Infrastrukturen, wie etwa Atomkraftanlagen, nun erlaubt seien. Dies könnte eine Reaktion auf die vergangenen Strafverfolgungsmaßnahmen sein, die schwerwiegende Folgen hatten.

Internationale Maßnahmen wie Operation Checkmate gegen BlackSuit verdeutlichen die zunehmende Koordination von Strafverfolgungsbehörden. Gleichzeitig deuten Aktivitäten von Gruppen wie Storm-2603 in China oder CyberVolk in Russland eine wachsende Nähe zwischen staatlichen und kriminellen Strukturen zumindest an. Erschwerend kommt hinzu, dass physische Einschüchterung und Gewalt – sowohl gegenüber Opfern als auch innerhalb der Szene – immer häufiger als Druckmittel eingesetzt werden.
Auf geopolitischer Ebene verschieben sich die Kräfteverhältnisse weiter in Richtung Offensive. Berichten zufolge investieren die USA und Polen verstärkt in offensive Cyberfähigkeiten, während diplomatische Initiativen an Gewicht verlieren. Auch Unternehmen wie Google erweitern ihre aktiven Abwehrmaßnahmen, was die Debatte um digitale „Letters of Marque“ neu belebt.

Zugleich wird der Umgang mit Ransomware-Zahlungen zunehmend politisiert. In Ohio wird über Genehmigungspflichten für Zahlungen lokaler Behörden diskutiert. Der Fall Jaguar Land Rover, bei dem angeblich eine passende Versicherung fehlte, wirft die Frage auf, ob staatliche Finanzhilfen im Schadensfall ein sinnvoller Ausweg sind, oder ob sie Kriminellen letztlich nur zusätzliche Anreize bieten. Auch in Teilen als Folge hiervon verlagert sich der Fokus auf weniger, aber finanziell lukrativere Angriffe, bei denen gezieltes Social Engineering gegen hochkarätige Opfer eine zentrale Rolle spielt.

Updates

EuRepoC informiert mit einem täglich kuratierten Cyber Incident Tracker über neu in die Datenbank aufgenommene Cybervorfälle. Diesen können Sie hier abonnieren.

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 Allianz SE gefördert.
Nähere Informationen zum EuRepoC-Projekt finden Sie hier.

Die DCSO

Die Auswertung wird unterstützt durch die Deutsche Cyber-Sicherheitsorganisation GmbH (DCSO). Der IT-Sicherheitsdienstleister wurde 2015 von der Allianz, Bayer, BASF und Volkswagen als Gemeinschaftsunternehmen gegründet.

Über die Autor:innen

Jakob Bund ist Wissenschaftler an der Stiftung Wissenschaft und Politik (SWP).

Lena Rottinger ist akademische Mitarbeiterin am Institut für Politische Wissenschaft (IPW) der Universität Heidelberg.

Kerstin Zettl-Schabath ist Senior Cyber Threat Analyst bei der Deutschen Cyber-Sicherheitsorganisation GmbH (DCSO).

Follow us on social media

@EuRepoC

linkedin/EuRepoC

contact@eurepoc.eu

https://eurepoc.eu