European
Repository of
Cyber Incidents

EuRepoC Cyberkonflikt Briefing

Q4 2025

Kerstin Zettl-Schabath
Jonas Hemmelskamp
Lena Rottinger

Beobachtungen zur Gesamtlage

Insgesamt wurden im vierten Quartal (Q4) 2025 **mit 207 neuen Cyber-Operationen etwa 9.2 Prozent weniger Operationen** in die EuRepoC-Datenbank aufgenommen als im dritten Quartal (Q3). Trotz des leichten Rückgangs liegt diese Zahl weiter deutlich über den Quartalswerten des zweiten Halbjahres 2024 sowie des ersten Halbjahres 2025 und um 21 Operationen über dem langfristigen durch EuRepoC durchschnittlich verzeichneten Quartalsdurchschnitt von 186 erfassten Operationen.

Die **durchschnittliche Intensität** der im Quartal erfassten Operationen beträgt 3.13 und liegt somit weiter über dem historischen Durchschnitt (2.94), zugleich jedoch leicht unterhalb der relativ hohen Intensität im dritten Quartal (3.24). Im kurzfristigen Trend nimmt die durchschnittliche Intensität der aufgenommenen Vorfälle entsprechend etwas ab.

Über das Briefing

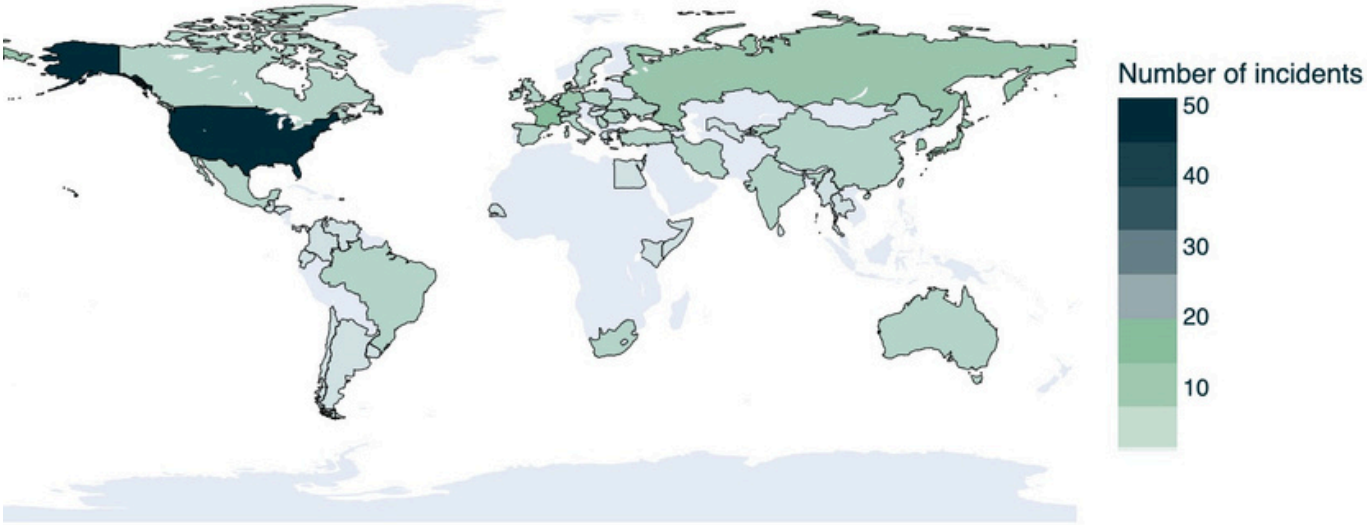
Das Cyberkonflikt-Briefing fasst die zentralen Trends, Dynamiken und Befunde zu den vom European Repository of Cyber Incidents (EuRepoC) in einem bestimmten Quartal erfassten Cyberoperationen zusammen. Diese müssen nicht notwendigerweise im Q4 2025 stattgefunden haben, sondern können bereits zu einem früheren Zeitpunkt begonnen haben. Dabei stehen technische, politische sowie rechtliche Aspekte im Vordergrund. Nähere Informationen zum EuRepoC-Projekt finden Sie hier.

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.

Weitere Informationen finden Sie unter https://eurepoc.eu

Geografische Verteilung von Cyberoperationen im 4. Quartal 2025



Regionale Trends

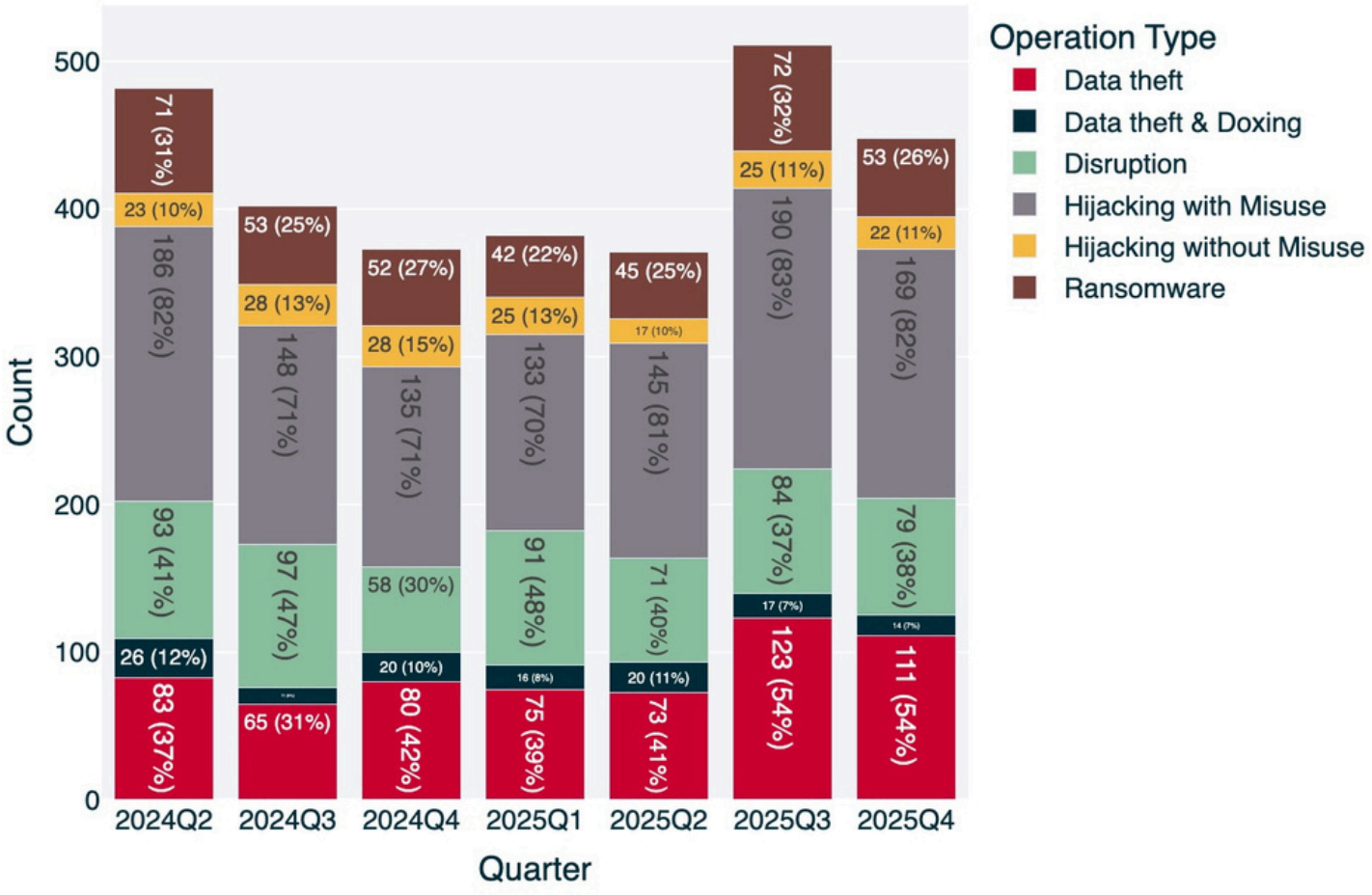
Mit 51 Operationen sind auch in diesem Quartal die USA der am häufigsten betroffener Staat. Die 27 EU-Mitgliedsstaaten sind in der aggregierten Betrachtung mit 59 Vorfällen aber noch häufiger ein Ziel von Operationen geworden als die USA. Das ist für EU-Mitgliedsstaaten der höchste Quartalswert seit dem letzten Höhepunkt im zweiten Quartal 2024 (61). Besonders in den Monaten November (25) und Dezember (20) 2025 wurde für EU-Mitgliedsstaaten jeweils eine im Trend vergleichsweise höhere Zahl von neuen Operationen aufgenommen.

In der Einzelbetrachtung folgen im vierten Quartal auf die USA Frankreich (15), Deutschland (11) und Südkorea (9). Besonders für Frankreich wurden allein seit Anfang Dezember zehn neue Operationen aufgenommen, wobei der doppelte Angriff auf La Poste durch NoName057(16) zwischen den Jahren im Dezember und Januar die wohl größten Wellen schlug.

Ähnlich hohe Wellen hat in Südkorea der Hack von Korea Telecom (KT) im August geschlagen. In der Folge gab es im vierten Quartal für Südkorea ungewöhnlich viele Vorfälle im Bereich der kritischen Infrastrukturen zu verzeichnen. Bei einigen dieser Operationen werden nordkoreanische Akteure wie die Lazarus Gruppe als Täter vermutet. Das IT-Sicherheitsunternehmen Bitdefender identifiziert ebenfalls einen ungewöhnlichen Anstieg von Ransomware-Aktivitäten in Südkorea seit September 2025, die das Unternehmen auf die sogenannte “Korean Leaks” Kampagne mit Qilin Ransomware zurückführt. Hierbei besteht der Verdacht, dass die nordkoreanische staatliche Gruppe Moonstone Sleet in der Affiliate-Rolle die Dienste des Ransomware-as-a-Service (RaaS) Anbieters Qilin in Anspruch nimmt, wodurch kriminelle und staatlich-affiliierte Handlungen weiter verschwimmen.

Die relative Verteilung der Operationstypen ist im Vergleich zum dritten Quartal konsistent geblieben. Der größte Anteil der aufgenommenen Operationen fällt mit 169 Fällen (82 Prozent) in die Kategorie

Verteilung der Arten von Cyberoperationen



Note: Individual cyber incidents may have several operation types in combination

“Hijacking with Misuse”. Diese Kategorie wird in der Regel im Zusammenspiel mit weiteren Kategorien (wie Disruption oder Spionage) erfasst. In den 12 Fällen, in denen sie alleinsteht, haben die Angreifer in Q4 eines von zwei Zielen: Diebstahl oder Defacement.

Krypto-Diebstahl und Defacement

Ein besonders attraktives Ziel für Defacements und Krypto-Diebstahl sind Organisationen, die auf den Handel mit Kryptowährungen und im Umgang mit dezentralisierten Finanzprotokollen (DeFi) spezialisiert sind. Ab August wurde eine Schwachstelle im BetterBank DeFi-Protokoll ausgenutzt, um Assets im Wert von 5 Millionen US-Dollar zu stehlen. Im November wurde eine Sicherheitslücke im DeFi-Protokoll der Handelsplattform Balancer gezielt verwendet, um Werte von über 100 Millionen US-Dollar aus Smart-Contracts zu entwenden.

Weitere Anlagewerte im Wert von 33 Millionen Euro gingen schließlich Ende November bei einem Hack der Südkoreanischen Kryptobörse Upbit verloren. Laut südkoreanischen Medienberichten vermuten Regierungsvertreter die Lazarus-Gruppe hinter dem Vorfall bei Upbit – schon wieder. Das wäre bereits der zweite erfolgreiche Lazarus Angriff von Upbit nach dem ähnlichen Hack von 2019.

Auch für einen Vorfall im September beim Japanischen Crypto-Miner SBI besteht seitens der Ermittler der Verdacht, dass nordkoreanische Akteure die Verantwortung tragen. Nach wie vor sind Angriffe auf diese Organisationen oftmals eine Finanzierungsquelle für den nordkoreanischen Staat.

Ebenfalls in die Kategorie “Hijacking with Misuse” fällt die Verunstaltung mehrerer Websites (Defacement). Im Oktober wurden zum Beispiel die Websites von vier Flughäfen in den USA und Kanada kompromittiert und mit Nachrichten versehen, die die Hamas unterstützen sollten und Beleidigungen gegen Donald Trump und Benjamin Netanyahu enthielten. Im November wurden schließlich mehrere Regierungswebsites in Kenya übernommen und mit “White-Supprematist” Nachrichten versehen.

Spionage
Der zweithäufigste Operationstyp war “Data theft”-Operationen (54 Prozent). Das Repositorium hat 111 Operationen von diesem Typ erfasst. Diese Operationen lassen sich gliedern in Ransomware-Angriffe mit sogenannter Double-Extortion Strategie, wobei die Daten nicht nur verschlüsselt, sondern auch gestohlen werden und in Angriffe, die gezielt dem Datendiebstahl dienen.

Auch im vierten Quartal wurde eine signifikante Anzahl von reinen Spionageoperationen und längerfristigen Spionagekampagnen durch chinesische Akteure aufgenommen. Für insgesamt 16 erfasste Spionageoperationen liegt eine Attribution vor, die chinesische Akteure verantwortlich macht. Zum Vergleich: An der zweiten Stelle steht Russland mit vier Operationen. Diese Zahlen müssen aber mit 39 nicht attribuierten reinen Spionageoperationen im Quartal kontrastiert werden.

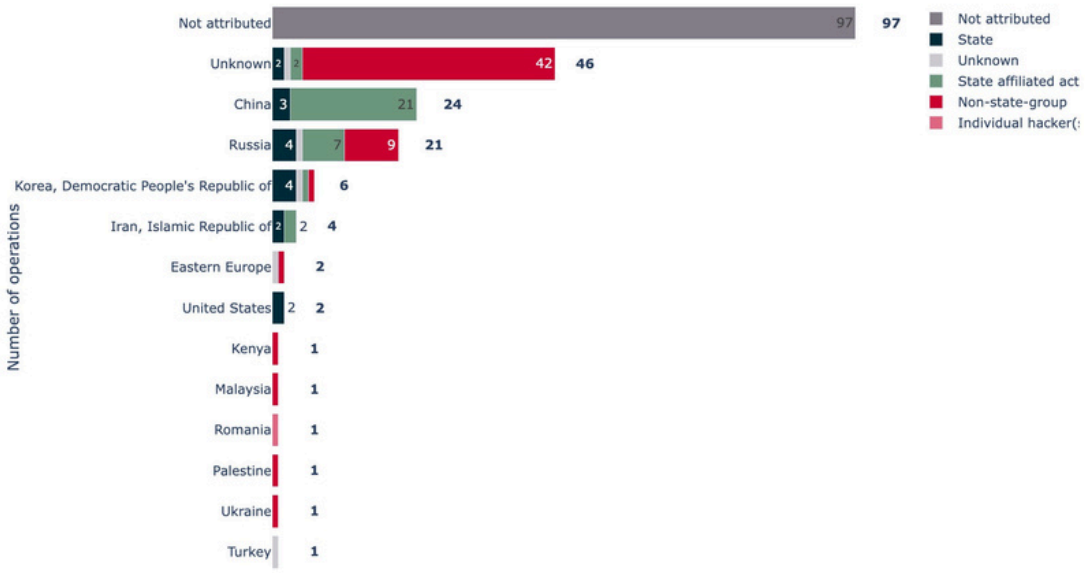
Die erfassten langfristigen chinesische Spionagekampagnen zielten dagegen wie schon in Q3 auf viele verschiedene geografische Räume ab. Ein großer Anteil davon fokussiert sich auf Staaten im Asiatischen Raum. Zugleich spionierte MustangPanda aber Europäische Diplomaten aus, während PhantomTaurus dasselbe für Botschaften im Mittleren Osten, Afrika und Asien tat, Kampagnen der Gruppen JewelBug sowie SaltTyphoon in Lateinamerika entdeckt wurden und die mit dem Chinesischen Ministerium für Staatssicherheit (MSS) verbundene Gruppe APT31 seit mindestens 2022 auch im russischen Technologiesektor spioniert . Ein besonderer Fokus der chinesischen Akteure sind dabei weiterhin Telekommunikationsausstatter wie F5 oder LG Uplus sowie Lösungen von Citrix oder Cisco und im Spezifischen eine größere Zahl von Angriffen auf Exchange Server weltweit. Ein häufig verwendeter Angriffsvektor ist in diesem Kontext nach wie vor die Ausnutzung der N-Day Schwachstelle ToolShell.

Einen leichten Rückgang gab es im relativen Anteil der politisch relevanten Ransomware-Operationen von dem in Q3 sehr hohen Anteil von 32 Prozent zurück zu langfristig üblicheren 26 Prozent in Q4.

Angreiferprofile und Attributionen

Im 4. Quartal sind 47 Prozent der bekannt gewordenen Vorfälle (noch) nicht attribuiert, während 28 Prozent von nicht-staatlichen bzw. individuellen Hacker(gruppen) ausgingen und 15 Prozent staatlich-unterstützen und 8 Prozent staatlichen Bedrohungsakteuren zugeordnet wurden.

Mutmaßliche Herkunftsländer der Initiatoren im 4. Quartal 2025



China, Russland, Nordkorea und der Iran führen dabei die Liste der Länder an, aus denen die Cyberoperationen durchgeführt wurden.

Fast ein Viertel aller Cybervorfälle aus dem Quartal sind dabei auf chinesische Bedrohungsakteure zurückzuführen, die größtenteils als staatlich unterstützt und staatliche Akteure klassifiziert wurden. Laut Medienberichten werden hinter dem weitreichenden Hack des US-Netzwerkausrüsters F5 staatliche chinesische Akteure vermutet. Selbiges gilt für den Angriff auf das Budget-Büro des US-Kongress während des Shutdowns, die vielberichtete AI-basierte Kampagne der Chinesischen Gruppe GTG-1002 gegen 30 Einrichtungen der kritischen Infrastruktur weltweit und für den Vorfall beim Britischen Außenministerium für den Medienberichten zufolge der chinesische Akteur STORM-1849 verantwortlich gemacht wird.

Ein auffälliges Muster zeigt sich auch bei der Frage, wer genau die zahlreichen chinesischen Angriffe hauptsächlich aufgedeckt und attribuiert hat, in Q4 waren das zu über 80% IT-Unternehmen. Politische Reaktionen auf chinesische Cybervorfälle blieben weitestgehend aus, nur die britische Regierung sanktionierte am 9. Dezember 2025 zwei chinesische Unternehmen (i-Soon and Integrity Tech) für deren "rücksichtslose und verantwortungslose Cyberaktivitäten". Bemerkenswert war vor allem das Schweigen von US Präsident Donald Trumps trotz wiederholter chinesischer Angriffe auf US-Institutionen und Kritische Infrastrukturbetreiber, dass nicht nur als Zeichen von Schwäche gewertet werden kann, sondern Chinas vorsätzlich schädliches Verhalten im Cyberraum zunehmend normalisiert. Das Ausbleiben politischer Reaktionen muss gleichzeitig im Kontext des sechswöchigen Regierungsstillstands im Herbst 2025 verstanden werden, der die Arbeit vieler US-Behörden stark einschränkte.

Ein deutlich anderes Bild zeigt sich im Fall russischer Bedrohungsakteure, die für 21 Cybervorfälle in Q4 verantwortlich gemacht wurden. Zu russischen Cyberaktivitäten äußerten sich gleich mehrere westliche Regierungen. Am 9. Dezember 2025 kündigte das US-Justizministerium rechtliche Maßnahmen gegen zwei "staatlich unterstützte cyberkriminelle Hackergruppen", namentlich CyberArmyofRussa_Reborn (CARR/Z-Pentest) und NoName057(16) an. In zwei Anklageschriften wird der Ukrainerin Victoria Eduardovna Dubravna vorgeworfen Cyberoperationen gegen kritische Infrastrukturen im Einklang mit Russlands geopolitischen Interessen durchgeführt zu haben. Dabei unterscheidet die Anklageschrift das Ausmaß staatlicher Verwicklung bei den Bedrohungsakteuren in "staatlich-unterstützend" für CARR und "staatlich geduldet" für NoName057(16). Diese Anklageschrift stellt damit das erste politisch signifikante Statement dar, bei dem der Gruppierung NoName057(16) eine Verbindung zum russischen Staat bewiesen wurde. Laut Anklageschrift sei NoName057(16) ein verdecktes Projekt, das von mehreren Angestellten des Zentrums für die Erforschung und Netzwerküberwachung des Jugendumfelds (CISM). Das CISM wurde 2018 auf Anordnung des russischen Präsidenten ins Leben gerufen. Während NoName057(16) bislang primär DDoS-Angriffe auf politische Institutionen durchführte, ist die Gruppe CARR/Z-Pentest durch den Angriff auf den norwegischen Damm im April 2025 bekannt geworden.

Neben der Anklageschrift, veröffentliche CISA noch ein Joint Advisory gemeinsam mit dreizehn verbündeten Staaten nach der im Juli durchgeführten Operation Eastwood. Das Joint Advisory bewertet die Angriffe von CARR und NoName057(16) als "weniger komplex und mit geringeren Auswirkungen" als Operationen von Advanced Persistent Threat (APT) Gruppierungen. In Q4 war vor allem Dänemark von NoName057(16)-Angriffen betroffen, die insbesondere im Kontext dänischer Kommunalwahlen im November 2025 stattgefunden haben. Die dänischen Behörden beteiligten sich nicht am Joint Advisory, sondern machten Russland in einem unabhängigen Statement verantwortlich für die November-Vorfälle sowie den Angriff von CARR/Z-Pentest auf ein dänisches Wasserwerk 2024. Auch die dänische Attribution hebt die Verbindung von NoName057(16) zum russischen Staat hervor und bestellte als öffentliche Konsequenz den russischen Botschafter ein.

Die deutsche Bundesregierung äußerte sich ebenfalls zu russischen Cyberangriffen. Anders als in der zeitnahen Reaktion von Dänemark, reagierten die Behörden aber erst anderthalb Jahre nach dem Vorfall. Am 12 Dezember 2025 hat die Bundesregierung den Angriff gegen die Deutsche Flugsicherung im August 2024 offiziell der russischen Hackergruppe APT28 auch bekannt unter den Namen „Fancy Bear" zugeordnet. Nachrichtendienstliche Datenauswertungen beweisen laut der Erklärung des Auswärtigen Amts eine direkte Verbindung dieser Gruppe zum militärischen Nachrichtendienst Russlands (GRU).

Entwicklungen rund um das Ökosystem der Cyberkriminalität

In Q4 setzten sich zahlreiche Trends des Cybercrime-Ökosystems fort, zugleich wurden jedoch neue Entwicklungen erkennbar, die 2026 prägen könnten. Das vor allem aus Jugendlichen bestehende Hacker-Kollektiv Scattered LAPSUS$ Hunters hatte in den Monaten zuvor durch

zahlreiche Angriffe auf große Unternehmen, insbesondere in Großbritannien, für Aufsehen gesorgt. Auch in Q4 gab es Meldungen von besonders jungen Menschen, die in kriminelle Aktionen verwickelt waren: In London wurden zwei Jugendliche verhaftet, die eine Kindertagesstätte gehackt und erpresst hatten. Noch konfrontativer agierten Scattered LAPSUS$ Hunters selbst: Diese sollen Informationen über US-Regierungsbeamte veröffentlicht haben, nachdem mexikanische Kartelle Berichten zufolge zuvor eine Belohnung hierfür ausgerufen hatten. Ob verstärkter Strafverfolgungsdruck auf die jugendlichen Täter – die im Gegensatz zu den meisten etablierten Ransomware-Gruppen in europäischen Ländern oder den USA ansässig sind – zu weniger riskanten Handlungen führen wird, bleibt abzuwarten.

Ein weiteres E-Crime-Phänomen, das in Europa bislang weniger Beachtung findet, aber international, insbesondere von den USA und China, stark bekämpft wird, ist das aus Südostasien stammende Scamming westlicher und auch chinesischer Personen, etwa durch sogenanntes „Pig Butchering“. In Q4 wurden zahlreiche Sanktionen, Anklagen und Urteile gegen die maßgeblich verantwortlichen Gruppierungen, wie die Prince Group und deren CEO, erhoben. Die US-Regierung richtete hierfür eigens eine Task Force ein, was angesichts der 2025 aufgelösten Anti-Desinformation Units die Prioritäten der Trump-Administration verdeutlicht. Zahlen zu deutschen oder europäischen Opfern sind bislang schwer zu ermitteln, da die Dunkelziffer hier oft noch höher ist als bei Ransomware.

Im Ransomware-Bereich stieg die Zahl der verzeichneten Opfer laut der Plattform *ransomware.live* auch im November und Dezember 2025 wieder deutlich an. Als aktivster Ransomware-as-a-Service (RaaS)-Provider etablierte sich Qilin weiterhin, die Gruppe stammt vermutlich aus dem russischen Raum. Zwar konzentriert sich die Strafverfolgung nach wie vor auf einige wenige Gruppen, die den Großteil der Aktivitäten ausmachen, jedoch bleibt abzuwarten, ob die zunehmende Fragmentierung der Szene die Effektivität dieser Maßnahmen beeinträchtigt. Analysten berichten etwa von „One-Man“-RaaS, die mit wenig Aufwand eigene Ransomware-Varianten entwickeln und vermarkten.

Auch Qilin war Kunde von BearHost, einem großen russischen Bulletproof-Web-Hosting-Provider, der Ende 2025 „aus politischen Gründen“ sein Geschäft einstellte – ohne Kunden zu entschädigen oder ihnen Zugriff auf ihre Server zu gewähren. Aus Deutschland operierende Rechenzentrumsdienste wurden zuletzt etwa von der Insikt Group mit diesen “high-risk hosting networks” in Verbindung gebracht, die bezichtigt werden, maliziöse Infrastruktur zu hosten.

Weitere Entwicklungen im Bereich Ransomware umfassen:

- **Zunehmender Missbrauch legitimer Tools**: Open-Source-DFIR-Tools wie Velociraptor, Nezha RMM und TruffleHog sowie Plattformen wie Dropbox und OneDrive, aber auch KI-gestützte Produktivitätstools werden missbraucht, um Erkennung zu umgehen und Daten zu exfiltrieren.
- **Verbesserte Verschlüsselung**: Die RansomHouse-Gruppe verwendet nun zwei Schlüssel pro Datei (Haupt- und Sekundärschlüssel), was die Entschlüsselung deutlich erschwert.
- **VPNs als Hauptzugang**: Laut At-Bay haben sich VPNs in den letzten fünf Jahren als primärer Einstiegspunkt für

Ransomware etabliert, während RDP abnahm. Besonders Cisco- und Citrix-VPNs sind anfällig.

- **Infostealer und Initial-Access-Broker treiben Ransomware-Aktivitäten weiter voran**. Internationale Strafverfolgung, etwa durch die letzte Iteration der „Operation Endgame“, erzielte zwar zeitweise Erfolge gegen Akteure wie LummaStealer, DanaBot oder Rhadamanthys, konnte jedoch keinen dauerhaften Erfolg erzielen, da einige bereits in neuen Versionen zurückkehrten. Zahlreiche „Low-Hanging-Fruits“ bleiben bestehen, etwa unveränderte Server der MedusaLocker-Ransomwaregang, da Kriminelle ihre Operational Security oft erst nach Vorfällen verbessern.
- **Veränderte „Kosten-Nutzen“-Logik beim Erwerb und der Nutzung von Zero-Day-Exploits**: Während diese früher vor allem staatlichen Akteuren für langjährige Spionageoperationen „vorbehalten“ waren, nutzen mittlerweile auch immer mehr Ransomware-Gangs diese, teilweise „lediglich“ für Datendiebstahl, oft auch zur Erpressung von Kunden der kompromittierten Software-Hersteller.

Auffällig waren zudem vermehrte Meldungen zu Cybersicherheitsvorfällen, die von Insidern der Zielorganisation oder von eigentlich mit Cybersicherheit betrauten Stellen verursacht oder begünstigt wurden. So bekannten sich zwei US-Cybersicherheitsexperten schuldig, selbst Ransomware gegen Unternehmen eingesetzt zu haben. In einem weiteren Fall entließ Crowdstrike einen Mitarbeiter, der Informationen an Scattered LAPSUS$ Hunters weitergegeben hatte. Auch in Q4 kam es zu „Racheakten“ entlassener Mitarbeiter gegen ihre ehemaligen Arbeitgeber, wobei oft noch bestehende Accountzugänge als Einfallstor dienen. Auch 2026 dürfte die „Bedrohung von innen“ weiterhin relevant bleiben, nicht zuletzt aufgrund anhaltender wirtschaftlicher Herausforderungen in Deutschland und Europa, die entsprechende Anreize für (entlassene) Mitarbeiter verstärken könnten. Aufgrund gestiegener Fluktuation ist auch weiterhin von Spearphishing-Kampagnen auszugehen, die auf Recruiting- und Bewerbungsprozesse abzielen. Dabei kommen sowohl nichtstaatliche als auch staatlich affiliierte Akteure infrage, etwa aus Nordkorea, dem Iran, aber auch Vietnam. Das nordkoreanische Regime hat Berichten zufolge allein 2025 über zwei Milliarden US-Dollar durch Ransomware, Kryptodiebstahl und die Infiltration von Unternehmen mit Fake-Remote-Mitarbeitern erwirtschaftet. Cybercrime bleibt damit auch für Staaten ein attraktives Mittel zur Finanzierung trotz Sanktionen.

Mehr von EuRepoC

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

About the authors

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

Jonas Hemmelskamp ist Chef-Datenanalyst ("Chief Data Scientist") für das EuRepoC-Projekt und Doktorand an der Universität Heidelberg.

Lena Rottinger ist Masterabsolventin der Universität Heidelberg und ist wissenschaftliche Mitarbeiterin im EuRepoC-Projekt; sie ist verantwortlich für die politische Kodierung von Cybervorfällen.

Follow us on social media


@EuRepoC


linkedin/EuRepoC


contact@eurepoc.eu


https://eurepoc.eu