EuRepoC

ADVANCED PERSISTENT THREAT Profile

Conti/Wizard Spider

Auch bekannt als

- **Conti** (VMware)
- **Wizard Spider** (Crowd-Strike)
- **ITG23** (IBM X-Force)
- **G0102** (MITRE ATT&CK)

Quellen: [1][2][3]

Herkunftsland

Operationszeitraum

2019-2022

Wizard Spider ist seit 2016 aktiv; die Conti Ransomware wurde im Dezember 2019 zum ersten Mal gesichtet. Aufgegeben hat die Gruppe ihre Infrastruktur, als das US-amerikanische Außenministerium im Mai 2022 eine Belohnung von 10 Millionen Dollar für Informationen ausgesetzt hatte, die zur Identifizierung oder Lokalisierung der Gruppenmitgliedern führen würden. Seitdem wird vermutet, dass Wizard Spieder sich in verschiedene Gruppen umorganisiert hat, darunter möglicherweise BlackByte, BlackBasta und Karakurt.
Quellen: [2][4][8][9]

Politische Zugehörigkeit

Vor dem Krieg in der Ukraine wurde die Gruppe von Experten "weithin als halbautonome Einrichtung des russischen Geheimdienstes angesehen", da sich ihre Aktivitäten mit den russischen Sicherheitsinteressen deckten. Nach dem Einmarsch in die Ukraine im Frühjahr 2022 bekannte sich Conti öffentlich zur russischen Regierung, ruderte jedoch zurück als sie damit auf erhebliche Kritik stieß. Die Enthüllung von Dokumenten im Februar 2022 deuten darauf hin, dass zwischen einigen Gruppenmitgliedern und dem russischen Inlandsgeheimdienst (FSB) informelle Verbindungen bestanden. Quellen: [4][5][6]

By Kerstin Zettl-Schabath , Lena Rottinger und Camille Borrett

November 2022

Akteurstyp

Vom Staat geduldete Cyberkriminelle, nationalistische Motive. Ein Bericht der IBM Security X-Force vom Juli 2022 stellte fest, dass die Gruppe nach dem russischen Einmarsch gezielt ukrainische Einrichtungen angegriff.
Quellen: [2][6][10]

Häufige Angriffsziele:

- **Australien**
- **Bahamas**
- **Kanada**
- **Costa Rica**
- **Frankreich**
- **Deutschland**
- **Indien**
- **Irland**
- **Italien**
- **Japan**
- **Mexiko**
- **Neuseeland**
- **Spanien**
- **Schweiz**
- **Taiwan**
- **Großbritannien**
- **Ukraine** (since 2022)
- **USA**

Nach den veröffentlichten Datenlecks zu urteilen, griff Conti mit seinen Ransomware-Operationen fast 800 Organisationen in 40 Ländern an. Die meisten Opfer befanden sich in den Bereichen Fertigung, Rechtsberatung und professionelle Dienstleistungen, Bau und Technik sowie im Einzelhandel. Nach Beobachtungen des Cybersicherheitsunternehmens Mandiant, könnte der hohe Anteil nordamerikanischer Ziele (60 %) auf ein auf Nordamerika ausgerichtetes Angriffsmuster hinweisen. Quellen: [7][10][12]

Gruppenzusammensetzung/Organisationsstruktur

Die in Russland ansässige Cyber-Kriminalitätsgruppe betrieb ein Ransomware-as-a-Service-Geschäftsmodell und beschäftigte mehrere Partner, die das Eindringen in die Netzwerke ihrer Opfer und die Verschlüsselung von Dateien überwachten. In der Regel wurden russischsprachige Partner in Foren auf der Grundlage ihrer Erfahrung, ihres Rufs und ihres Aktivitätsniveaus rekrutiert. Einige zahlten Conti eine Provision zwischen 10 und 30 % der erhaltenen Lösegeldzahlungen; andere schienen Teil eines Gehaltsystems zu sein. Die Gruppe arbeitete regelmäßig mit anderen Ransomware-Gangs wie Maze, LockBit 2.0 und Ragnar Locker zusammen. Im August 2021 veröffentlichte ein ehemaliges Conti-Mitglied namens "m1Geelka" vertrauliche Information über die Organisation, Ausbildung und Führungsstruktur der Gruppe. Die Online-Identitäten einiger Teammitglieder waren bereits zuvor offengelegt worden, darunter der Anführer/Projektleiter ("reshaev" alias "cybergangster"), der Conti-Administrator ("Tokyo"), ein Assistent und ein Anwerber ("IT-Work").

Die Gruppe bekannte sich nach dem Einmarsch in die Ukraine öffentlich zur russischen Regierung, was zu Unmut führte: sowohl innerhalb der Gruppe (unter ukrainischen Mitgliedern und russischen, die die Ukraine unterstützen) als auch bei anderen Bedrohungsakteuren (meist anderen Cyberkriminellen), die in der Einmischung in politischen Fragen ein Geschäftsrisiko sahen. Nach dieser Diskussion beschloss eines der Mitglieder der Conti-Gruppe, private Conti-Chatprotokolle und andere interne Informationen zu veröffentlichen. Das Bekenntnis führte dazu, dass Staaten Conti mit dem russischen Staat in Zusammenhang brachten und die Gruppe mit strengen Sanktionen belegte, die als Reaktion auf den Angriff auf die Ukraine verhängt wurden. Damit lief jedes Opfer, das eine Lösegeldzahlung an eine bestimmte Person oder Einrichtung leistete, einschließlich sanktionierter Finanzinstitutionen zur Abwicklung der Transaktion, Gefahr gegen Sanktionen zu verstoßen. In den USA kann ein einziger Verstoß gegen die Sanktionsbestimmungen zu Geldstrafen von bis zu 1 Million Dollar und einer 20-jährigen

Haftstrafe führen. Obwohl die Gruppe versuchte ihr Bekenntnis herunterzuspielen, verursachte die Verkündung irreparablen Schaden für das operatives Geschäft und ihre Reputation. Am 19. Mai 2022 wurden Hauptbestandteile der Infrastruktur zum Hochladen von Daten des Opfers und zur Abwicklung von Zahlungsvorgängen abgeschaltet.

Sicherheitsexperten von AdvIntel beobachteten im Nachgang bei einer Reihe ehemaliger Conti-Partner einen Anstieg an Aktivitäten, was auf eine Dezentralisierung hindeutet, die sich während der Umstrukturierung der Kernakteure von der starken vertikale Hierarchie von Conti verabschiedet. BlackByte, BlackBasta und Kara-kurt sind einige der mutmaßlichen Ableger, die im Mittelpunkt dieser Umstrukturierung stehen. Quellen: [4][11][17][19][23][24]

Auswirkungen

Direkt

- **Finanzielle Folgen** (Conti hat mehr als 1000 Opfer angegriffen und bis Januar 2021 über 150 Millionen Dollar eingenommen; durchschnittliche Conti-Lösegeldzahlung: 480.333 Dollar [Mai 2022])
- **Auswirkungen auf operatives Geschäft** (die durchschnittliche Dauer eines Conti-Ransomware-Angriffs beträgt 15 Tage)

Indirekt

- **Reputationsverlust** (z. B. für die neu gewählte Regierung von Costa Rica während/nach der Angriffswelle im April 2022)

Quellen: [11][13]

Angriffsart(en)

- **Ransomware**
- **Datendiebstahl & Doxxing**

Quellen: [2][11]

Bedrohungsindex

7/24 mittelschwere Bedrohung

Index scoring scale

Score	Label
≤6	Geringe
>6 - ≤12	Mittelschwere
>12 - ≤18	Hohe
>18 – 24	Sehr hohe

Der Bedrohungsindikator ist abgeleitet aus dem EuRepoC Datensatz 1.0. Er stellt einen zusammengesetzten Kennwert dar, der fünf Teilindikatoren in sich vereint: die **sektorale** und **geographische** Ausdehnung der APT-Angriffe, der **Schweregrad** der Angriffe, die **Häufigkeit** der Angriffe und der Einsatz von **Zero-Days**. Zu beachten ist, dass nur Angriffe berücksichtigt werden, die der APT-Gruppe während ihres Operationszeitraums öffentlich zugeschrieben wurden und die spezifischen EuRepoC-Kriterien entsprechen. Die Punktzahlen berücksichtigen die Praxis weiterer APT-Gruppen, die von EuRepoC

analysiert werden, da die Schwellenwerte für die Bestimmung niedriger und hoher Punktzahlen auf der Bandbreite der Punktzahlen mehrerer APT-Gruppen beruhen. Ausführliche Information zur Methodik, die dem Index zugrunde liegt, finden Sie hier.

Aufschlüsselung der Punktzahl für Conti/Wizard Spider:

Teilindikator	Punktzahl	Erklärung
Schweregrad der Angriffe	2 /5	Dieser Teilindikator stellt einen Durchschnittswert der "gewichteten Cyber-Intensität" aus dem EuRepoC-Codebuch dar, der aus allen Angriffen berechnet wird, die dem APT im Operationszeitraum zugeschrieben werden. Bewertet wird die Angriffsart, ihre potenziellen physischen Auswirkungen und ihre gesellschaftspolitische Tragweite - weitere Informationen finden Sie hier.
Sektorale Ausdehnung der Angriffe	2 /8	Dieser Teilindikator berechnet die durchschnittliche Anzahl der angegriffenen Sektoren jedes Angriffes, der den APT-Gruppen über ihren Operationszeitraum zugeschrieben wurde. Wenn die Mehrheit der angegriffenen Sektoren für das Funktionieren der Zielgesellschaften kritisch ist (z.B. politische System oder kritische Infrastrukturen), wird ein Multiplikator angewandt. Im Durchschnitt zielten die Angriffe, die Conti/Wizard Spider in der EuRepoC-Datenbank zugeschrieben werden, auf einen Sektor ab. Da jedoch alle Angriffe gegen politische Systeme und/oder kritische Infrastrukturen gerichtet waren, wurde die Punktzahl mit dem Faktor 2 multipliziert.
Geografische Ausdehnung der Angriffe	1 /4	Dieser Teilindikator berücksichtigt die durchschnittliche Anzahl der betroffenen Länder aller Angriffe, die der APT-Gruppe zugeschrieben werden. Ganze Regionen oder Kontinente, die von einem Angriff betroffen sind, werden höher gewichtet. Im Fall von Conti/Wizard Spider waren bei den Angriffen, die der Gruppe in der EuRepoC-Datenbank zugeschrieben werden, im Durchschnitt jeweils nur ein Land betroffen.
Häufigkeit der Angriffe	2 /4	Dieser Teilindikator wird berechnet, indem die Gesamtzahl der Angriffe, die der APT-Gruppe in der EuRepoC-Datenbank zugeschrieben werden, durch die Anzahl der aktiven Jahre der APT-Gruppe dividiert wird. Die erhaltenen Werte werden dann auf eine vierstufige Skala umgerechnet. Im Durchschnitt wurde Conti/Wizard Spider für weniger als einen Angriff pro Jahr verantwortlich gemacht (0,67).
Nutzung von Zero days	0 /3	Dieser Indikator berechnet den Prozentsatz der Angriffe, die der APT zugeschrieben werden und einen oder mehrere Zero-Days einsetzen. Die erhaltene Punktzahl wird dann in eine dreistufige Skala umgewandelt. Bei keinem der Angriffe, die der Conti-Gruppe zugeschrieben werden, wurden Zero-Days verwendet.

→ Insgesamt erhält Conti/Wizard Spider im Vergleich zu anderen APT-Gruppen eine moderate Bedrohungsbewertung. Die im Rahmen von EuRepoC analysierten Angriffe richteten sich im Durchschnitt jeweils auf wenige Länder und Sektoren. Darüber hinaus wurden bei der Gruppe zugeschriebenen Angriffe keine Zero-Days missbraucht.

TECHNISCHE MERKMALE / EIGENHEITEN / AUSGEREIFTHEIT

Die Gruppe betreibt ein Ransomware-as-a-Service (RaaS)-Geschäftsmodell und stellt ein digitales Verwaltungssystem für ihre Partner (andere Bedrohungsakteure/Kriminelle) bereit. Als halbautomatischer recovery-Dienstleister nutzt die Gruppe automatische Netzwerkscans um lohnende Ziele zu identifizieren, indem sie sich über kompromittierte Netzwerke ausbreitet und alle Gerät und Konten auf dem Weg dahin verschlüsselt. Im Allgemeinen nutzt Conti viele frei verfügbare Technologien, die oft für legitime Zwecke entwickelt wurden (z. B. Cobalt Strike, AnyDesk, Atera oder Tor) und von der Gruppe für kriminelle Zwecke missbraucht werden. Wie andere Ransomware-Bedrohungsakteure wendet die Gruppe eine doppelte Erpressungstaktik an, die mit der Freigabe vertraulicher Daten droht und gleichzeitig das Netzwerk eines Opfers erkundet, wenn die erste Lösegeldforderung zur Entschlüsselung der Zielsysteme nicht erfüllt wird. Conti ist ein sehr ausgereifter Bedrohungsakteur, was sich auch in den Geschäftspraktiken der Gruppe widerspiegelt, z. B. in ihren Geldwäschetechniken.

Grundlegende Angriffsmuster

Conti änderte und aktualisierte sein Angriffsmuster fast täglich, indem es Exploits für kürzlich entdeckte Softwarefehler verwendete und die verspätete Bereitstellung von Patches ausnutzte, um noch anfällige Netzwerke anzugreifen. Innerhalb dieser Abweichungen bei der Ausführung, lässt sich ein grundlegendes Angriffsmuster identifizieren:

(1) Zielauswahl (beobachtete Techniken: Phishing, massenhaftes Scannen von Schwachstellen, High-End-Software zur Verbreitung von Schadsoftware, Credential Stuffing, gefälschte Websites, Identitätsvortäuschung)

(2) Einsatz und Durchführung (Installation von Hintertüren, Identifizierung geschäftskritischer Systeme wie Domänencontroller oder Backup-Server, Exfiltration von Daten)

(3) Verschlüsselung der Daten des Opfers (mit zufällig erzeugten Schlüsseln)

(4) Übermittlung der Forderung und Einleitung von Verhandlungen (Übermittlung einer Lösegeldforderung, Bereitstellung von Kommunikationsmitteln für Verhandlungen)

Zero-Day Schwachstellen

Conti nutzte in der Regel bekannte Sicherheitslücken. Doch Ende 2020 setzte die Gruppe eine gekaufte Zero-Day-Schwachstelle im Internet Explorer 11 ein.

Verwendete Malware (nicht abschließend)

Conti v3.0	Trickbot	Emotet
BazarLoader	ColbaltStrike	Ryuk
ICEDID		

Quellen [11] [14] [15] [16]

Auswahl von Taktiken und Techniken anhand des MITRE ATT&CK Framework, die von der Gruppe eingesetzt werden

MITRE Initial Access

External Remote Services
Phishing
Spearphishing attachment
Spearphishing link
Valid Accounts

MITRE Persistence

Boot or logon autostart execution
Create or modify system process
Scheduled task/job
Valid Accounts

MITRE Defense Evasion

File and directory permissions modification
Impair Defenses
Indicator removal
Masquerading
Modify Registry
Obfuscated files or information
Process injection
Subvert trust controls
Valid Accounts

MITRE Exfiltration

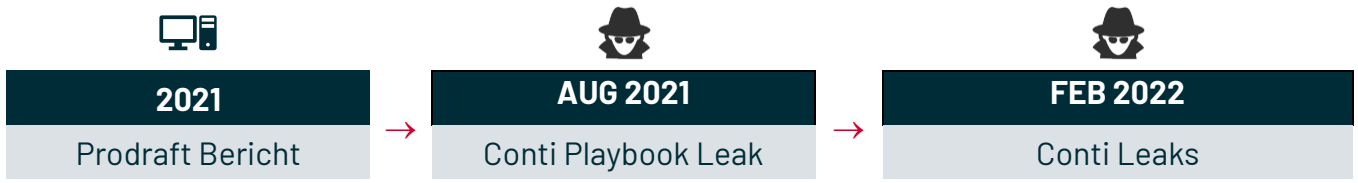
Exfiltration over alternative protocol
Exfiltration over C2 channel

MITRE Impact

Data encrypted for impact
Service Stop

ATTRIBUTION

Attributions-Meilensteine



Quellen: [11] [17] [18]

Attributionskontroversen

Wizard Spider/Conti und Ryuk: CrowdStrike führt die Operationen mit den Schadsoftware Conti und Ryuk auf dieselbe profilierte und ausgereifte Cyberkriminalitätsgruppe Wizard Spider zurück. Andere Experten betrachten Conti und Ryuk als zwei getrennte Bedrohungsakteure, die sehr ähnliche Muster in der Ransomware und Bitcoin-Geldbörsen verwenden, was auf eine Verbindung zwischen beiden Gruppen hindeutet. Die Ransomware von Conti scheint eine Fortsetzung der Ransomware Ryuk zu sein. Ein leitender Conti-Mitarbeiter (Senior Manager) hatte offenbar Kontakt und Zugang zu mehreren Mitgliedern von Ryuk. Dies ist ein anschauliches Beispiel für die häufige Unklarheit bei der Unterscheidung von Bedrohungsakteuren und Schadsoftwaremustern, insbesondere da sich kriminelle Gruppen neu organisieren um der Strafverfolgung zu entgehen.

Conti und UNC1756: Der Bedrohungsakteur, der hinter dem Einsatz der Conti-Ransomware gegen die Regierung von Costa Rica im April stand, bezeichnete sich selbst bei der Ankündigung der Operation als UNC1756. Die Abkürzung UNC – die für uncategorised (nicht kategorisiert) steht - ist eine Anspielung auf die von Mandiant verwendete Bezeichnung für Hackergruppen, die noch nicht klar identifiziert werden können. Dass der Angriff von UNC1756 unterzeichnet und Aktualisierungen über die Dark-Web-PR-Seite von Conti veröffentlicht wurde, haben Zweifel daran aufkommen lassen, ob die Führung von Conti die Arbeit einer angegliederten Gruppe hervorhob, oder ob UNC1756 ein gezielter Versuch war Strafverfolgungsbehörden und Sicherheitsexperten mit einer gefälschten Identität irrezuführen.

Conti und Maze: Die Forscher von Intel 471 fanden in den Codes von Conti kopierte Komponenten aus der Maze-Malware. Berichten zufolge standen führende Conti-Entwickler in engem Kontakt mit Maze-Entwicklern, als die Conti-Schadstsoftware selbst noch in der Entwicklung war.

Quellen: [2] [5] [11] [19] [20]

Attributions-/ Erkennungsempfindlichkeit

Conti ist bekannt für seine Widerstandsfähigkeit und die schnelle Übernahme neuer Techniken und Taktiken. Die Gruppe passte ihre Angriffsmuster fast täglich an. Vermutet wird jedoch, dass es keine Reaktion auf bestimmte Attributionen war, sondern eine Präventivstrategie, um nicht entdeckt zu werden. Darüber hinaus setzte die Gruppe verschiedene Verschleierungstechniken und wöchentliche Codeänderungen ein, um Schadsoftware-Analysesysteme zu umgehen. Quellen: [2] [11]

RECHTLICHE UND POLITISCHE MASSNAHMEN, DIE GEGEN DIE GRUPPE ERGRIFFEN WURDEN

Politische/juristische Maßnahmen und Strafverfolgung

Am 6. Mai 2022 kündigte das US-amerikanische Außenministerium eine Belohnung in Höhe von 10 Millionen US-Dollar für Informationen über die Mittäter der Conti-Ransomware im Rahmen des Programms "Rewards for Justice" an, das ursprünglich als Initiative zur Terrorismusbekämpfung eingeführt wurde. Quellen: [13][21][22]

Angeklagte Personen / sanktionierte ("zugehörige") Einrichtungen

Keine Personen angeklagt (Stand: November 2022)

Bedeutende Operationen

Abschaltung des irischen Gesundheitswesens 2021:
Die irische Gesundheitsbehörde (Health Service Executive) wurde von einem großen Conti-Ransomware-Angriff getroffen, der einige medizinische Behandlungen unterbrochen hat.

Der Ransomware-Angriff von Conti auf Costa Rica 2022:
Conti brach während eines Regierungswechsel in mehrere staatliche Einrichtungen und Behörden ein und forderte 10 Millionen Dollar Lösegeld. Der neue Präsident, Rodrigo Chaves, rief daraufhin den nationalen Notstand aus. Die Gruppe veröffentlichte schließlich 97 % der Daten, die sie von costaricanischen Organisationen gestohlen hatte.
Quellen: [4][5][25]

QUELLEN

[1] Baskin (2020), *TAU Threat Discovery: Conti Ransomware*, VMware Security Blog. Online verfügbar unter: https://blogs.vmware.com/security/2020/07/tau-threat-discovery-conti-ransomware.html [abgerufen am: 29.11.2022]

[2] Das CrowdStrike Intel Team (2020), *WIZARD SPIDER Update: Resilient, Reactive and Resolute*, Crowdstrike Blog. Online verfügbar unter: https://www.crowdstrike.com/blog/wizard-spider-adversary-update/ [abgerufen am: 29.11.2022]

[3] Villadsen und Hammond (2021), *Trickbot Rising – Gang Doubles Down on Infection Efforts to Amass Network Footholds*, Security Intelligence. Online verfügbar unter: https://securityintelligence.com/posts/trickbot-gang-doubles-down-enterprise-infection/ [Abgerufen am: 29.11.2022]

[4] Bogusalvskiy und Kremez (2022), *DisCONTInued: The End of Conti's Brand Marks New Chapter For Cybercrime Landscape*, AdvIntel. Online verfügbar unter: https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape [abgerufen am: 29.11.2022]

[5] Ferrett (2022), *Conti Attack on Costa Rica: Who is UNC1756?*, Searchlight Security. Online verfügbar unter: https://www.slcyber.io/blog/conti-attack-on-costa-rica-who-is-unc1756 [abgerufen am: 29.11.2022]

[6] Burgess (2022), *Leaked Ransomware Docs Show Conti Helping Putin From The Shadows*, Wired. Online verfügbar unter: https://www.wired.co.uk/article/conti-ransomware-russia [abgerufen am: 29.11.2022]

[7] Mandiant (2022), *Keeping up with CONTI*, Mandiant. Online verfügbar unter: https://www.mandiant.com/resources/conti-ransomware [abgerufen am: 29.11.2022]

[8] Naeem (2022), *CONTI*, MITRE ATT&CK. Online verfügbar unter: https://attack.mitre.org/software/S0575/ [abgerufen am: 29.11.2022]

[9] Cyble Team (2021), *Conti Ransomware Resurfaces, Targeting Government & Large Organizations*, Cyble Blog. Online verfügbar unter: https://blog.cyble.com/2021/01/21/conti-ransomware-resurfaces-targeting-government-large-organizations/ [abgerufen am: 29.11.2022]

[10] Villadsen et al. (2022), *Unprecedented Shift: The Trickbot Group is Systemically Attacking Ukraine*, Security Intelligence. Online verfügbar unter: https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine/ [abgerufen am: 29.11.2022]

[11] PTI Team (2021), *Conti Ransomware Group In-Depth Analysis*, Prodaft: Proactive Defense Against Future Threats. Online verfügbar unter: https://www.prodaft.com/m/reports/Conti_TLPWHITE_v1.6_WVcSEtc.pdf [abgerufen am: 29.11.2022]

[12] Unit 42 Team (2022), *Conti-Ransomware*, Unit 42. Online verfügbar unter: https://unit42.paloaltonetworks.com/atoms/conti-ransomware/ [abgerufen am: 29.11.2022]

[13] Gatlan (2022), *US Offers $15 Million Reward for Info on Conti Ransomware Gang*, BleepingComputer. Online verfügbar unter: https://www.bleepingcomputer.com/news/security/us-offers-15-million-reward-for-info-on-conti-ransomware-gang/ [abgerufen am: 29.11.2022]

[14] CISA, FBI, und NSA (2022), *Joint Cybersecurity Advisory: Conti Ransomware*, CISA. Online verfügbar unter: https://www.cisa.gov/uscert/sites/default/files/publications/AA21-265A-Conti_Ransomware_TLP_WHITE.pdf [abgerufen am: 29.11.2022]

[15] Comeau (2022), *The Conti Ransomware Leaks: Six Takeaways*, Tech Decisions. Online verfügbar unter: https://my-techdecisions.com/network-security/conti-ransomware-leaks/ [abgerufen am: 29.11.2022]

[16] Millington und Gayda (2020), *Wizard Spider*, MITRE ATT&CK. Online verfügbar unter: https://attack.mitre.org/groups/G0102/ [abgerufen am: 29.11.2022]

[17] Abrams (2021), *Angry Conti Ransomware Affiliate Leaks Gang's Attack Playbook*, BleepingComputer. Online verfügbar unter: https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/ [abgerufen am: 29.11.2022]

[18] Fokker und Tologonov (2022), *Conti Leaks: Examining the Panama Papers of Ransomware*, Trellix. Online verfügbar unter: https://www.trellix.com/en-us/about/newsroom/stories/research/conti-leaks-examining-the-panama-papers-of-ransomware.html [abgerufen am: 29.11.2022]

[19] Intel 471 Team (2022), *Cybercrime Loves Company: Conti cooperated with other ransomware gangs*, Intel 471. Online verfügbar unter: https://intel471.com/blog/conti-ransomware-cooperation-maze-lockbit-ragnar-locker [abgerufen am: 29.11.2022]

[20] Hanel und Stone-Gross (2019), *WIZARD SPIDER Adds New Features to Ryuk for Targeting Hosts on LAN*, Crowdstrike Blog. Online verfügbar unter: https://www.crowdstrike.com/blog/wizard-spider-adds-new-feature-to-ryuk-ransomware/ [abgerufen am: 29.11.2022]

[21] Price (2022), *Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice*, United States Department of State. Online verfügbar unter: https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/ [abgerufen am: 29.11.2022]

[22] Rewards for Justice (2022), *Conti*, US State Department. Online verfügbar unter: https://rewardsforjustice.net/rewards/conti/ [abgerufen am: 29.11.2022]

[23] Sulkin und Schaetzel (2022), *Ransomware Response Complicated by Growing Number of Sanctions in Wake of Russian Invasion of Ukraine*, Benesch: Data Meets World. Online verfügbar unter: https://www.datameets-world.com/blog/ransomware-response-complicated-by-growing-number-of-sanctions-in-wake-of-russian-invasion-of-ukraine [abgerufen am: 29.11.2022]

[24] Office of Foreign Assets Control (2021), *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, Department of the Treasury. Online verfügbar unter: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf [abgerufen am: 29.11.2022]

[25] Sharma (2022), *Costa Rica Declares National Emergency After Conti Ransomware Attacks*, BleepingComputer. Online verfügbar unter: https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/ [abgerufen am: 29.11.2022]

Die Berechnungen für den Bedrohungsindex-Indikator basieren auf der Version 1.0 der EuRepoC-Datenbank, die hier heruntergeladen werden kann:
https://strapi.eurepoc.eu/uploads/Eu_Repo_C_Global_Database_1_0_22d4a4aee7.xlsx

Zuletzt aktualisiert: 30.11.2022