INTELLIGENCE ȘI CULTURA DE SECURITATE

CONFERINȚA STIINȚIFICĂ STUDENȚEASCĂ
CONFERENCE PROCEEDINGS

VOLUMUL 4
2025

Editura Academiei Naționale de Informații
„Mihai Viteazul”

INTELLIGENCE
ȘI CULTURA DE SECURITATE

nr. 4 – 2025

– Conferința Științifică Studențească –

Editura Academiei Naţionale de Informaţii „Mihai Viteazul”

Bucureşti, 2025

Editura Academiei Naţionale de Informaţii „Mihai Viteazul”
© ANIMV
Bucureşti, 2025
Telefon: 0377720.000/1216
Fax: 0377721.134; 0377721.125
ISSN 2972 – 1350 ISSN-L 2971 – 8139

CUPRINS

CÂND ATACATORII DEVIN VICTIME: VULNERABILITĂȚILE GRUPĂRILOR DE CRIMINALITATE CIBERNETICĂ

Claudia-Alecsandra GABRIAN*

Abstract:

Ransomware groups represent a category of the cybercriminal landscape, they operate anonymously, through aliases and underground channels, but since 2022, when the war between Russia and Ukraine started, the cybercriminal ecosystem has seen some changes. Information leaks have shown that although these groups seem unstoppable, on the contrary, they are vulnerable and make mistakes. This article highlights vulnerabilities of cybercrime groups, based on the leak of internal data from two notable ransomware groups: Conti and Black Basta. The primary scope is to analyze how the leaks occurred, what they reveal about the internal operations of cybercriminal activities, and why such intelligence is highly valuable for cybersecurity research.

Conti was the first ransomware group that supported Russia in the context of the invasion in Ukraine, the leaks in 2022 revealed internal discussions, strategies, financial transactions, aliases, organizational structure, etc. After this major event, in 2025, another ransomware group was involved in a leak, Black Basta, that was highly active in this field since Conti shut down its activity. The leaks exposed critical operational details, names, chats, victims, transactions, etc. This article is relevant in this field because it represents a key topic about cybercrime vulnerabilities.

Conti and Black Basta leaks represent the two most important information leakage events within groups, and justify that cybercrime groups are also susceptible to the same exploits they exploit in others. The leaks offer valuable information and a unique opportunity to analyze cybercrime from the inside, their recruitment, and even internal conflicts. Knowing the weaknesses of cybercrime groups represents a significant way to understand how they think and organize their attacks.

Cuvinte-cheie: CONTI, BlackBasta, Telegram, leaks, cyber-attacks, ransomware

Introducere

Grupările de criminalitate cibernetică sunt considerate ca fiind foarte bine organizate, extrem de sofisticate şi de cele mai multe ori membrii grupărilor nu comit greşeli care să conducă la identificarea acestora. Pseudonimele şi tiparul pe care le folosesc sunt singurele care

* Universitatea Babeş-Bolyai, Facultatea de Istorie şi Filosofie, Departamentul de Studii Internaţionale şi Istorie Contemporană, Cluj-Napoca, claudia.gabrian@ubbcluj.ro.

pot să fie asociate cu o operaţiune specifică. În mediul de criminalitate cibernetică numărul grupărilor de ransomware active în prezent este de peste 60 de grupări, dintre care 16 au apărut după data de 1 ianuarie 2025 (Rapid7, 2025). Acest număr este foarte relevant, deoarece tendința de apariție a acestor tipuri de grupări este în continuă creștere. Mediul de ameninţări cibernetice devine unul foarte volatil şi complex, astfel, creşterea semnificativă poate fi atribuită şi faptului că există grupări care se rebranduiesc, în special după acţiuni de aplicare a legii împotriva acestora.

O tendinţă care este mai vizibilă din anul 2022 este aceea potrivit căreia unii dintre cei mai relevanţi actori de pe scena ameninţărilor cibernetice devin, la rândul lor, victime ale unor breşe de securitate, chiar probabil trădări interne, expuneri neintenţionate, sau chiar obişnuinţă, iar situaţia celor două grupări, Conti şi Black Basta confirmă acest paradox. Dacă se au în vedere scurgeri masive de date interne, conflicte între membrii sau erori operaţionale, aceste grupări de criminalitate cibernetică demonstrează faptul că nimeni nu este imun în faţa vulnerabilităţilor cibernetice, fie ele de natură umană sau tehnică, nici măcar cei care le exploatează zi de zi.

Scopul acestui articol este de analizare a modului în care publicarea informaţiilor din interiorul grupărilor poate să reprezinte un pas important în identificarea membrilor unei grupări. De asemenea, articolul îşi propune şi analizarea relevanţei pe care aceste scurgeri le au în domeniul cercetării ecosistemului de criminalitate cibernetică, prin înțelegerea dinamicii şi a fragilităţii acestor grupări. În cadrul cercetării se vor analiza documente interne şi discuţii între membrii grupării, rolul acestora fiind de a observa activitatea membrilor din aceste grupări de ransomware. Chat-uri interne ale grupărilor Conti şi Black Basta au fost postate pe X (fostul Twitter în 2022) şi pe canalul de Telegram (în 2025) şi pe Dark Web. Au fost utilizate aceste surse pentru a se înțelege mai bine modul de acţiune al acestor grupări, strategiile interne şi chiar posibilitatea asocierii unor nume adevărate cu aceste alias-uri şi parteneriate dintre aceste grupări şi servicii de informaţii din Rusia.

Prezenta cercetare investighează vulnerabilităţile interne ale grupărilor de criminalitate cibernetică, adresând un hiatus în literatura de specialitate prin valorificarea datelor provenite din scurgerile de informaţii din interiorul Conti şi Black Basta. Analiza acestor două incidente, considerate repere fundamentale în peisajul ameninţărilor actuale, fundamentează o nouă metodă de explorare a vulnerabilităţilor acestora, fiind cele mai relevante expuneri de informaţii care au fost

publicate vreodată. Analiza scurgerilor de date evidenţiază un proces critic de destabilizare operaţională şi structurală. În cazul Conti, fragmentarea a fost accelerată de disensiunile geopolitice interne, iar în cazul Black Basta, incidentul a fost precedat de încălcarea unui protocol intern de non-agresiune.

Metodologia utilizată în această cercetare este una calitativă, fiind bazată pe metoda netnografiei şi strategia studiului de caz. Prin metoda netnografiei s-au analizat scurgerile de informaţii publicate pe Telegram @ExploitWhispers; X (ex-Twitter) @ContiLeaks, cât şi interacţiunile online ale membrilor acestor grupări prin canale private, cum ar fi Matrix. Complementar, strategia studiului de caz a facilitat investigarea aprofundată şi contextualizată a grupărilor Conti şi Black Basta, corelându-se datele empirice cu dinamica lor organizaţională specifică. Prin aceste două metode, s-au identificat tipare comportamentale şi vulnerabilităţi structurale recurente.

Întrebarea de cercetare: În ce mod contribuie informaţiile provenite din breşele interne la procesul de deanonimizare a membrilor şi la înţelegerea structurii organizaţionale a grupărilor Conti şi Black Basta?

Rezultate

Criminalitatea cibernetică este un termen general care descrie multitudinea de activităţi infracţionale desfăşurate utilizând un computer, o reţea sau un alt set de dispozitive digitale. Există o gamă largă de activităţi ilegale pe care infractorii cibernetici le comit, dintre care se numără şi atacul de tip ransomware, printre multe altele. Criminalitatea cibernetică nu cunoaşte limite fizice, poate să ia multe forme şi evoluează încontinuu. Acest tip de ameninţare afectează atât persoanele fizice, companii şi entităţi guvernamentale, ceea ce poate duce la pierderi financiare semnificative. Activitatea lor se întinde pe diverse platforme şi tehnologii digitale, iar atacul de tip ransomware este un tip de malware care criptează datele critice ale victimelor, cerând o răscumpărare. Dacă această plată este făcută, victimele primesc o cheie de decriptare pentru a recupera accesul. Din punct de vedere financiar, atacurile ransomware duc la pierderi de date şi active. Există multe cazuri de ransomware care au avut succes, cele mai afectate sectoare sunt cele sănătate, educaţie, energie, transporturi etc. (ProofPoint, 2024).

Gruparea Conti

Gruparea Conti a fost una dintre cele mai sofisticate, agresive și eficiente operațiuni ransomware, vizând multe companii importante și organizații guvernamentale. Conti a apărut pentru prima dată la sfârșitul anului 2019, devenind una dintre operațiunile predominante de *ransomware-as-a-service* (RaaS). În urma analizării mai multor rapoarte despre această grupare, se sugerează o legătură cu un alt ransomware, cunoscut sub numele Ryuk, care era condus de un grup rusesc de criminalitate cibernetică cunoscut sub numele de Wizard Spider (CSO, 2022).

Conti deși opera ca un ransomware obișnuit, ceea ce îl diferenția de multe alte tipuri de ransomware era viteza sa de criptare, tehnicile avansate și utilizarea unui model de dublă extorcare, în care atacatorii nu numai că criptau fișierele, dar furau și datele sensibile, amenințându-i cu expunerea lor dacă nu se plătea răscumpărarea. În urma analizării discuțiilor dintre membrii, chiar dacă acea răscumpărare era plătită, ei nu asigurau integritatea datelor și nepublicarea lor online. Conti făcea parte din tendința crescândă a *ransomware-as-a-Service* (RaaS), care permitea afiliaților cu mai puțină expertiză tehnică să achiziționeze pachete de atac și să lanseze atacuri ransomware. Conti oferea acces la instrumentele și infrastructura lor în schimbul unei părți din plățile de răscumpărare. Acest model amplifica semnificativ numărul de atacuri efectuate de Conti, deoarece reducea barierele de acces pentru potențialii atacatori (Cyberly).

Motivul alegerii acestei grupări se datorează faptului că este prima grupare ransomware care a susținut invazia Rusiei în Ucraina. Aceasta și-a anunțat sprijinul deplin pentru guvernul rus și a amenințat cu atacuri cibernetice asupra infrastructurii critice a oricărei țări care va ataca Rusia. Astfel, în urma susținerii invaziei, au fost postate zeci de mii de mesaje, de către un cercetător în domeniul securității informatice care a avut acces la baza de date, oferind informații despre modul în care era condusă operațiunea, numele asociat membrilor, discuțiile cu victimele etc. După acest eveniment, membrii grupării au continuat să se implice în activități ilegale sub alte denumiri, cum ar fi o nouă operațiune ransomware numită Black Basta, care a reprezentat și continuarea activității acestora. Ca urmare, în 19 mai 2022, infrastructura Conti, inclusiv site-ul său oficial, au fost închise (CSO, 2022).

Gruparea Black Basta

Black Basta cunoscută pentru operațiunea de tip *ransomware-as-a-Service* (RaaS), a apărut în aprilie 2022 și este descendentul Conti și

Revil. A câştigat rapid notorietate pentru proliferarea sa rapidă, vizând peste 500 de organizaţii la nivel global în diverse sectoare de infrastructură critică, inclusiv în domeniul sănătăţii. Black Basta folosea un model de dublă extorcare, iar tacticile grupului vizau utilizarea instrumentelor legitime în scopuri rău intenţionate. Potenţialele legături cu Conti, au transformat gruparea într-o ameninţare semnificativă şi persistentă (TheSecMaster, 2025).

Apariţia acestei grupări a coincis cu declinul Conti, deşi o descendenţă directă nu a fost dovedită definitiv, poate fi posibil un rebranding sau o divizare a grupului. Mai mulţi factori sugerează o legătură puternică, cum ar fi asemănarea codului, multe dintre tacticile, tehnicile şi procedurile (TTP) ale Black Basta se aliniază cu cele utilizate de Conti, inclusiv dubla extorcare, direcţionarea unor industrii specifice şi utilizarea anumitor instrumente. Recrutarea de persoane din interior prin intermediul forumurilor de hacking (Exploit, XSS) relevă faptul că Black Basta îşi promova serviciile pe pieţele subterane ale criminalităţii cibernetice, indicând o operaţiune profesionistă care căuta mereu afiliaţi (TheSecMaster, 2025).

Originile exacte ale grupării sunt neclare, dar există mai multe indicii care relevă faptul că aceasta opera din Rusia sau din altă ţară din Europa de Est. Notele de răscumpărare şi alte comunicări ale grupării sunt în limba rusă sau conţin fragmente din limba rusă. O altă legătură relevantă, atât Conti, cât şi Black Basta folosesc bursa de criptomonede rusească Garantex pentru a spăla răscumpărările (Barracuda, 2024). Potrivit unei analize detaliate realizate de SentinelOne, operatorii Black Basta descurajează în mod activ atacurile asupra ţărilor din Comunitatea Statelor Independente (CSI), sau ţări prietene, care include majoritatea statelor din fosta URSS. Această practică este comună în rândul grupurilor de ransomware cu legături ruseşti, care evită să atace ţinte locale pentru a nu atrage atenţia autorităţilor (SentinelOne).

Chiar dacă s-a menţinut ca una dintre cele mai importante grupări de ransomware din ecosistemul de criminalitate cibernetică, scurgerea de informaţii din 11 februarie 2025 a expus vulnerabilitatea grupării, cât şi mecanismele interne, oferind o perspectivă concretă asupra tacticilor lor, la fel ca şi în cazul informaţiilor postate despre gruparea Conti (Kela, 2025). Colecţia de jurnale de chat interne utilizate de operatorii şi membrii Black Basta au fost cele mai relevante informaţii postate. Scurgerile conţineau aproximativ 200.000 de mesaje datate între 18 septembrie 2023 şi 28 septembrie 2024 (SRM, 2025).

Conti leaks

Informațiile din interiorul Conti au apărut pentru prima dată pe contul de Twitter numit „ContiLeaks" în data de 27 februarie 2022. Datele conţineau peste 60.000 de chat-uri interne de pe serverul privat de chat XMPP criptat şi Jabber, care se întind pe parcursul mai multor ani. Cel care a publicat informaţiile este de origine ucraineană, iar în urma analizei acestora, se identifică următoarele: structuri salariale, activităţi zilnice, structura grupului, adrese Bitcoin, fotografii ale serverelor de stocare şi un fişier ZIP protejat prin parolă care conţinea codul sursă pentru criptorul, decriptorul şi constructorul ransomware-ului Conti (Heimdal, 2024). Această divulgare de informaţii este considerată un eveniment notabil, în urma căreia se poate realiza o analiză concretă a operaţiunilor din interiorul unei grupări şi reprezintă un pas major prin care se poate atribui şi identifica membrii grupării (Trellix, 2022).

Jurnale Jabber postate sunt chat-uri individuale între fiecare doi membri. Prima parte conţine mesaje din 21 iunie 2020 până în 16 noiembrie 2020, în timp ce a doua parte conţine arhive din 29 ianuarie 2021 până în 27 februarie 2022, cu unele lacune. Scurgerea a inclus informaţii de la 6 servere Rocket.Chat diferite din perioada 31 august 2020 - 26 februarie 2022. În acest articol, s-au analizat conversaţiile membrilor extrase din jurnalele Jabber şi a folosit parţial conţinutul jurnalelor Rocket.Chat pentru a corobora constatările. La început, Jabber a fost folosit pentru mai multe tipuri de conversaţii, inclusiv atacuri continue. Spre 2021, majoritatea conversaţiilor tehnice (inclusiv piratarea anumitor companii, sarcini de codare etc.) au fost mutate pe Rocket.Chat (KELA, 2022).

În urma analizei chat-urilor interne în limba rusă, se identifică faptul că această grupare este organizată ca şi o companie obişnuită, având departamente pentru toate categoriile şi personal specializat (resurse umane, testeri, analişti OSINT, programatori, echipă de training, negociatori etc.). Aceştia îşi primesc salariul regulat în zilele de 15 şi 30 ale fiecărei luni, iar programul de lucru este între 10:00 şi 18:00, ora Moscovei, cinci zile pe săptămână (Trellix, 2022).

S-a identificat organigrama grupării, sunt 28 de membri, având toţi aliasuri: *Stern* este şeful principal, împreună cu *Tramp*. *Hof, Hors, Bentley, Starfall şi Zevs* sunt administratori de sistem, *Max* este developer Trickbot (botnet- platformă de distribuţie ransomware), *Revers* este hacker şi manager, *Swift şi Dollar* sunt hackeri şi *Reshaev* este hacker de top. *Professor, Bio şi Pumba* se ocupă de negocierile pentru plată răscumpărărilor din partea companiilor. *Buza* este developer şi

teamleader/cercetător OSINT, *Skippy* se ocupă de resursele umane şi de partea legală, *Many, Pin, Paranoik* şi *Cybergangster* lucrează la cryptolocker, decriptează datele pentru victime. *Salamandra*, *Kagas, Viper, Elvira şi Ford* se ocupă doar de partea de resurse umane, *Jaime* este developer şi *Mango* este manager tehnic (FORESCOUT, 2022).

Informaţiile regăsite în chat-urile interne ne ajută să identificăm mai multe tipare şi metode de activitate, astfel: *Stern* este şeful care supraveghează totul şi are 100 de persoane pe statul de plată. *Salmon* care este recrutor, afirmă faptul că weekend-urile şi vacanţele trebuie să fie respectate. *Bentley* care este manager, a lucrat acolo timp de un an, dar compania există de peste 10 ani. Există posibilele conexiuni guvernamentale potrivit lui *Angelo* care este tester/coder, *Stern* (un alt membru) este strâns afiliat cu FSB sau alte structuri şi lucrează pentru „Pu". Este important de menţionat faptul că *Basil* care este tester/coder a fost întrebat dacă este de la FSB, acesta a răspuns ulterior că are informaţii serioase legate de activitatea de la frontiera ucraineană. Această declaraţie a fost făcută cu şapte zile înainte de incursiunea Rusiei în Ucraina, ceea ce poate să sugereze faptul că gruparea are o relaţie apropiată cu guvernul rus şi/sau acţionează în interesul acestuia (Trellix, 2022). Unii membri ai grupului stăteau într-un birou din Rusia, pe baza conversaţiilor lor legate de comandarea mâncării şi întâlnirile într-un cadru real (KELA, 2022).

Printre alte departamente, Conti avea o echipă de apelanţi, un apelant trebuia să aibă cunoştinţe solide de limba engleză vorbită (nivel B2-C1) şi să aibă vârsta cuprinsă între 18 şi 25 de ani. Aceştia erau recrutaţi de echipa de resurse umane a Conti pentru a lucra de la distanţă pentru „un magazin online" în străinătate. Apelanţii câştigau mai mult în funcţie de succesul unui apel, programul de lucru era între 18:00-2:00, ora Moscovei (corespunzând programului obişnuit de lucru din emisfera occidentală) şi primeau concediu plătit, dar nu aveau încheiat niciun contract oficial conform Codului Muncii (Trellix, 2022).

Black Basta leaks

Scurgerile de informaţii Black Basta au avut loc pe 11 februarie 2025 şi au oferit o perspectivă profundă, nu doar asupra conflictelor interne ale grupului, ci şi asupra mecanismelor utilizate. S-a identificat faptul că există o tendinţă semnificativă care a fost verificată prin aceste jurnale de chat, aceea potrivit căreia grupările de ransomware reinvestesc răscumpărările plătite pentru a achiziţiona vulnerabilităţi zero-day (Rapid 7, 2025). O tehnică de atac zero-day este o eroare de

securitate pentru care furnizorul sistemului afectat nu a pus încă la dispoziția utilizatorilor afectați un patch pentru a remedia eroarea apărută (CSO, 2021).

Un administrator numit @ExploitWhispers al unui grup Telegram nou creat, „Шепот Басты" (Basta's Whisper) a distribuit conversațiile interne Matrix ale Black Basta, conținând peste 200.000 de mesaje. Administratorul a declarat că motivația din spatele scurgerii de informații a fost decizia unor membrii Black Basta de a „trece linia" atacând băncile ruseşti, o mişcare considerată inacceptabilă de către cel care a divulgat informațiile. Datele scurse au acoperit o perioadă cuprinsă între 18 septembrie 2023 și 28 septembrie 2024, în cadrul cărora au fost identificate informații sensibile, oferind o privire de ansamblu asupra funcționării interne Black Basta. Conținutul includea acreditări compromise, adrese IP, discuții operaționale interne, date despre victime, documente juridice, informații de plată, adrese de criptomonede și detalii despre infrastructura tehnică (KELA, 2025).

Deşi nu au fost identificate atacuri asupra băncilor ruseşti, identitatea și intenția lui @ExploitWhispers rămân neclare; ar putea fi un afiliat nemulțumit, un cercetător în domeniul securității sau un concurent al Black Basta RaaS. Potrivit lui @ExploitWhispers, liderul Black Basta, *GG, alias AA*, este un individ rus pe nume *Oleg Nefedov*. Pe baza cercetărilor din domeniul informațiilor open-source (OSINT), există un articol armean în care O. Nefedov a fost căutat de forțele de ordine din SUA și a fost reținut la Erevan pe 21.06.2024 și a scăpat în mod misterios de instanța armeană la două zile după arestarea sa (CIVILNET, 2024).

Prezentare generală a membrilor cheie și a dinamicii din cadrul BlackBasta este următoarea: *GG* (alias *Tramp)* este liderul de grup, *Lapa* este administrator cheie, *Cortes* este fost afiliat grupului Qakbot, *YY* este un alt administrator cheie al BlackBasta, *Bio* este un fost membru al lui Conti, iar când a lucrat cu Conti, Bio și-a schimbat porecla din „bio" în „pumba", dar de atunci a revenit la numele său original la BlackBasta. O altă descoperire relevantă are în vedere faptul că au fost identificate 533 de adrese IP din Rusia pentru atacurile lansate(FIRST, 2025). *Tinker* este implicat în acțiuni spam/vishing, este posibil să fi fost afiliat anterior și cu Conti. *Nickolas* este colaborator apropiat al lui *GG* în chat-ul „*talks.icu*". *N3auxaxl* este dezvoltator la distanță, posibil subordonat lui *YY*. *Ugway* este denumirea pentru operatori tehnici implicați în mai multe aspecte ale operațiunii, de la implementarea atacurilor, obținerea de acreditări, programe malware etc. (eSentire, 2025).

Cele mai relevante pasaje extrase din discuții arată că *GG* nu a trimis niciun mesaj între 20 iunie 2024 și 3 iulie 2024. Când *GG* și-a reluat

activitatea în chatul Matrix, a avut o conversaţie lungă cu un membru numit *Chuck*, discutând circumstanţele arestării sale, unde prietenii săi ruşi de la nivelul numărul 1 în stat au zburat imediat pentru a-l elibera. *Chuck* a întrebat dacă numărul 1 este „vvp" (potenţial V.V. Putin), însă nu a primit nicio confirmare sau infirmare. În plus, *Chuck* a menţionat o recompensă de 10 milioane de dolari pentru informaţii despre „tr" (posibil „-amp"), referindu-se posibil la recompensa americană pentru cinci membri cheie ai bandei Conti, inclusiv hackerul *Tramp*. În chat, *GG* a fost într-adevăr identificat drept *Tramp* (liderul Conti) prin „biografie" (cunoscut şi sub numele de „*pumba*", un alt membru Conti) (Trellix, 2025).

Mai mult, în timp ce discutau despre durata implicării lor în activităţi ilicite, *GG* şi *Chuck* au declarat că vor continua atât timp cât „bunicul" va trăi şi vor lucra până la încheierea Operaţiunii Militare Speciale (SMO), făcând referire la invazia Rusiei în Ucraina. Nu este clar la cine se referă „bunicul", însă ar putea fi o referire la o persoană de rang înalt care oferă protecţie liderilor Black Basta. *Chuck* a exprimat că SMO va dura o perioadă extinsă (Trellix, 2025). O altă descoperire este faptul că Black Basta utilizează ChatGPT pentru o varietate de scopuri, inclusiv compunerea de scrisori formale frauduloase în engleză, parafrazarea textului, rescrierea programelor malware şi colectarea datelor despre victime (Trellix, 2025).

Comunicarea ulterioară dintre *GG* şi *Chuck* se referă la un membru al grupului Conti/Trickbot, Fedor Andreev, care are Red Notice pe site-ul Interpolului. *GG* afirmă faptul că *Bentley*, unul dintre liderii Conti/ Trickbot, care este din Rusia, se presupune că lucrează pentru FSB. Din cauza unui atac legat de Black Basta RaaS, „biroul" îl căuta pe *GG*, acesta a răspuns întrebând „ce birou - FSB, FSO sau departamentul K?" (FSB: Serviciul Federal de Securitate, FSO: Serviciul Federal de Protecţie, Departamentul K: Departamentul Federal de Afaceri Interne care se ocupă de IT/criminalitate cibernetică). *Tinker* a dezvăluit că biroul era FSB. *GG* sub denumirea de "*usernamegg*" are două birouri în Moscova, unde îşi aveau sediul dezvoltatori şi operatori de programe malware (Trellix, 2025).

În urma analizării discuţiilor publicate online, au fost identificate următoarele elemente fundamentale referitoare la activitatea şi profilul operaţional al persoanei identificate sub pseudonimul *GG* (corelat cu identitatea lui *Tramp*, liderul grupării Conti). Primul element vizează beneficierea de o imunitate extrateritorială şi patronaj politic de nivel înalt, dedusă din capacitatea de a obţine un "coridor verde" pentru eliberarea sa rapidă în urma unei reţineri şi din referirile constante la protecţia oferită de figuri politice centrale. Al doilea element evidenţiază

alinierea ideologică și strategică la interesele geopolitice ale Federației Ruse, manifestată prin asumarea continuării operațiunilor până la finalizarea Operațiunii Militare Speciale și prin evitarea sistematică a vizării țărilor prietene. Al treilea element relavă o simbioză între structurile infracționale și agențiile de securitate statale (FSB, FSO), confirmată de prezența unor membri care activează dual sau sub supraveghere directă a "biroului".

Al patrulea element indică o instituționalizare fizică și logistică de tip corporativ, prin menținerea unor sedii administrative în Moscova, utilizarea unui personal auxiliar pentru securitatea transporturilor și implementarea unor protocoale stricte de acces și control ierarhic. Al cincilea element subliniază vulnerabilitatea strategică în fața contramăsurilor interne, reflectată prin eforturile de editare a mesajelor publice (de la pro-Rusia la pace) pentru a atenua represaliile internaționale. Toate aceste activități indică faptul că membrii grupării operează într-un cadru de criminalitate cibernetică hibridă, unde granița dintre infracționalitatea pură și obiectivele de securitate națională este deliberat ambiguizată (Interl417, 2025). Ca o evaluare, acest grad avansat de profesionalizare și protecție politică transformă gruparea dintr-un simplu actor de tip ransomware, într-o entitate de relevanță strategică, a cărei destabilizare este condiționată mai degrabă de dinamica politică internă a statului gazdă, decât de intervențiile tehnice ale agențiilor de securitate externe.

Interpretări

Analiza scurgerilor de informații despre chat-urile Conti și Black Basta a relevat potențiale conexiuni cu autoritățile ruse și colaborări cu alte operațiuni ransomware și malware. Chat-urile au arătat faptul că atât Black Basta, cât și Conti pot să fie localizate în Moscova, iar revizuirea scurgerilor de informații despre chat-urile Black Basta a demonstrat faptul că operațiunile nu s-au schimbat fundamental față de cele ale Conti. Conti și Black Basta au funcționat ca o companie bine organizată, cu mai multe locații fizice în Rusia, menținând diferite echipe de apelanți, negociatori, criptografi, coderi și spammeri. Aceste grupări au acționat sub convingerea că autoritățile ruse îi vor proteja de repercusiuni.

S-a observat faptul că unii afiliații Conti s-au alăturat Black Basta, astfel și legăturile au fost reconfigurate în noua grupare. De fiecare dată când are loc un rebranding pentru grupările ransomware, membrii se regrupează, învață din greșeli, dezvoltă instrumente inovatoare mai sofisticate (uneori datorită inteligenței artificiale) și continuă sub un

nume nou, atâta timp cât afacerea RaaS generează câştiguri financiare şi nu repetă ceea ce au făcut în trecut.

Chiar dacă operaţiunile grupării Conti au fost închise în 2022, continuarea activităţii infracţionale sub egida Black Basta este documentată prin analiza recentelor scurgeri de date, unde reiese faptul că le-a continuat. Acest caz relevă un proces extins de reflecţie internă asupra vulnerabilităţilor Conti, iar dezbaterile membrilor Black Basta privind infrastructura, reţelele de conexiuni şi instrumentele moştenite de la Conti, fundamentează ipoteza că noua entitate funcţionează ca un produs al evoluţiei organice a ecosistemului *ransomware-as-a-service* (RaaS). Aceste elemente relevă faptul că succesul operaţional al grupării este condiţionat de capacitatea de a asimila şi rectifica erorile strategice ale Conti, transformând informaţiile provenite din breşele interne, într-un potenţial spre reconfigurare structurală.

Analiza sugerează o constrângere majoră, abandonarea completă a paradigmelor operaţionale anterioare şi lansarea unui proiect RaaS complet autonom, rămân obiective dificil de atins, având în vedere că rădăcinile Black Basta sunt intrinsec legate de componentele tehnice ale grupării Conti. În secţiunea de interpretare, această dependenţă de parcurs, demonstrează faptul că grupările de criminalitate cibernetică nu pot opera o ruptură totală de propriul trecut organizaţional, fiind forţate să îşi reconstruiască reziliența pe aceeaşi arhitectură de bază, ceea ce menţine active direcţiile pentru cercetări viitoare.

O altă similaritate face referire la faptul că deşi infractorii cibernetici sunt motivaţi financiar şi au un istoric de colaborare transfrontalieră, adesea evitând implicarea în mediul politic, actualul conflict Rusia-Ucraina este menţionat în ambele chat-uri ale grupărilor şi nu trebuie să fie ignorat, mai ales faptul că în ambele grupări, membrii acestora menţionează faptul că au cunoştinţe de rang înalt din FSB. Deşi aceste afirmaţii nu au fost verificate independent, stabilirea unei legături directe între liderul unui grup ransomware şi serviciile secrete ruseşti ar fi o descoperire semnificativă. Statul rus oferă o impunitate controlată, atâta timp cât grupările nu vizează ţinte din interiorul Rusiei sau al CSI şi sunt dispuse să colaboreze cu serviciile de informaţii FSB, SVR la cerere, autorităţile în aceste condiţii pot ignora activitatea lor infracţională externă (DarkCovenant, 2023).

Cu toate acestea, presupusele legături ale liderului Black Basta cu serviciile secrete ruseşti ar putea sugera o relaţie mai profundă între grupările de ransomware şi serviciile de securitate ale statului, ridicând îngrijorări legate de securitatea naţională: în ce măsură a existat o colaborare între statul rus şi grupările Conti şi Black Basta? Aceasta

se justifică prin eliberarea lui *GG* din închisoare cu ajutor rusesc şi a discuţiilor purtate cu membrul *Chuck*, cât şi prin menţionarea instituţiilor de informaţii din Rusia şi legăturile dintre membrii grupărilor cu aceste instituţii. Întrebarea este relevantă, având în vedere istoricul grupării de a viza în mod explicit numeroase organizaţii de infrastructură critică din Europa. Conti şi Black Basta leaks au fost un rezultat direct al acestui conflict, deoarece au susţinut invazia Rusiei în Ucraina. Se poate concretiza o vulnerabilitate internă majoră, aceea potrivit căreia resursa umană reprezintă factorul care a declanşat închiderea definitivă a acestor două grupări.

Asemănările dintre Conti şi Black Basta sunt legate şi de faptul că ambele grupări au fost considerate printre cele mai sofisticate în perioada lor de ascensiune. Membrii păreau a fi veterani experimentaţi în ransomware şi criminalitate cibernetică, vorbitori de limbă rusă, scenariul demantelării operaţiunilor fiind aproape improbabil, chiar la doi ani diferenţă între ele.

Una dintre cele mai relevante informaţii regăsite, este legată de liderul grupării Black Basta, care este un cetăţean rus pe nume Oleg Evgenievich Nefedov, care a fost regăsit în cadrul grupării Conti, fiind asociat cu mai multe aliasuri *Tramp*, *Trump*, *GG* şi *AA*. Astfel, indică implicarea sa în grupări predecesoare majore, cum ar fi Conti. Deşi formarea de noi grupări este comună, iar cele deja închise apar adesea sub nume noi, aceste informaţii oferă dovezi suplimentare ale unor astfel de practici şi subliniază importanţa monitorizării comportamentelor afiliate în cadrul grupărilor ransomware.

Conexiunile între statul rus şi grupările de criminalitate cibernetică nu sunt neobişnuite, deoarece serviciile de informaţii ruseşti şi grupările de infractori cibernetici menţin în mod tradiţional relaţii de cooperare, primele bazându-se pe sprijin operaţional în cadrul unui acord *quid pro quo*: actorii clandestini îşi pot continua activitatea fără repercusiuni atâta timp cât cooperează cu statul. Fundamentul acestor relaţii este constrângerea infractorilor cibernetici să plătească bani în schimbul protecţiei, să participe la operaţiuni cibernetice organizate de stat, cum ar fi spionajul prin APT-uri sau furtul de date şi să susţină naraţiunile statului prin campanii hacktiviste sau de dezinformare.

Concluzii

Ransomware-ul reprezintă o ameninţare la adresa tuturor instituţiilor şi companiilor, iar Conti şi Black Basta reprezintă exemplele relevante pentru a justifica importanţa lor în ecosistemul de criminalitate

cibernetică. Grupările de ransomware sunt în continuă evoluţie, mai ales prin utilizarea inteligenţei artificiale, iar publicarea informaţiilor interne în cele două cazuri menţionate relevă importanţa studierii metodelor de atac şi a mentalităţii pe care aceşti atacatori o au. Utilizarea unui model de extorcare dublă, viteza de criptare şi tacticile sofisticate creează o variantă deosebit de periculoasă de ransomware.

Analiza datelor exfiltrate permite nu doar identificarea şi arestarea actorilor cheie din aceste grupări, ci şi clarificarea implicaţiilor şi motivaţiilor geopolitice. Sprijinul instituţional rus a ghidat activitatea acestor grupări pe parcursul ultimilor patru ani. Deşi succesiunea operativă de la Conti la Black Basta s-a încheiat formal la începutul anului 2025, riscul sistemic rămâne ridicat. Disoluţia unor astfel de organizaţii proliferează în realitate cu instabilitate, prin migrarea membrilor specializaţi către structuri emergente sau chiar prin reconfigurarea lor sub noi identităţi digitale.

Modelul RaaS, tacticile de dublă extorcare, adoptarea rapidă a noilor tehnici şi utilizarea instrumentelor legitime în scopuri rău intenţionate pot să reprezinte un punct de plecare în analizarea unei viitoare grupări de ransomware care va apărea sau care chiar a apărut în primăvara anului 2025, după închiderea activităţii Black Basta, conducând la identificarea unei noi organizări a membrilor Black Basta, ex-Conti. De asemenea, este important de urmărit dacă vor apărea alte scurgeri de informaţii care să ajute la identificarea membrilor grupării sau chiar să se analizeze modul în care aceştia vor fi mai precauţi cu membrii pe care îi acceptă.

Prin coroborarea datelor extrase din jurnalele de comunicaţii ale grupărilor Conti şi Black Basta, prezenta cercetare şi-a atins obiectivul fundamental, demonstrând faptul că publicarea informaţiilor din interiorul reţelelor de tip ransomware constituie un instrument critic în identificarea arhitecturii lor. Analiza a relevat faptul că aceste scurgeri de date nu sunt simple fragmente informaţionale, ci resurse strategice care permit cercetătorilor să cartografieze un ecosistem marcat de o fragilitate structurală surprinzătoare.

Răspunsul la întrebarea de cercetare indică faptul că breşele interne contribuie la procesul de deanonimizare şi înţelegere organizaţională prin trei mecanisme esenţiale: identificarea corelaţiilor dintre alias-uri (cum este cazul identificării lui *Tramp* ca lider central în ambele entităţi); expunerea fluxurilor financiare şi relevarea unei ierarhii de tip corporativ care mimează structurile comerciale legitime. Validarea empirică a acestor date confirmă faptul că înţelegerea structurii interne şi a motivaţiilor actorilor cheie oferă o perspectivă

unică asupra riscurilor hibride cu care se confruntă instituţiile de apărare şi securitate naţională.

Cercetarea demonstrează că operaţiunile acestor grupări nu sunt motivate exclusiv de profitul financiar, ci sunt profund influenţate de dinamica interpersonală complexă, presiunile politice externe şi simbioza cu serviciile de informaţii ale statului gazdă. Scurgerile de informaţii au permis creionarea unei organigrame detaliate, evidenţiind o specializare riguroasă a activităţii lor.

Lucrarea demonstrează că deşi grupări precum Conti şi Black Basta au părut invulnerabile în mediul digital, ele au funcţionat ca entităţi administrative cu vulnerabilităţi umane şi structurale majore, a căror transgresare a anonimatului prin breşe interne reprezintă cel mai eficient punct de acces pentru strategiile proactive de apărare şi deanonimizare a criminalităţii cibernetice organizate.

Direcţiile viitoare de cercetare se pot concentra pe investigaţii ştiinţifice aprofundate privind impactul acestor scurgeri de informaţii, asupra modului în care pot ajuta forţele de ordine să identifice persoanele care au stat în spatele atacurilor. În plan secund, este imperativă monitorizarea sistemică a ecosistemului infracţional, cât şi dinamica de reconfigurare a reţelelor emergente, analizând modul în care noile grupări de tip ransomware-as-a-service (RaaS) asimilează lecţiile învăţate din eşecurile Conti şi Black Basta pentru a-şi fortifica securitatea operaţională.

Contribuţia originală a prezentei lucrări rezidă în abordarea analitică a unui domeniu marcat de un deficit de date primare, propunând o perspectivă directă asupra dinamicii interne şi a interacţiunilor complexe din cadrul ecosistemelor de criminalitate cibernetică. Dezvoltarea unui cadru interpretativ a permis corelarea rezultatelor empirice cu identificarea vulnerabilităţilor structurale specifice grupărilor Conti şi Black Basta.

Bibliografie

1. Barracuda. 2024. „Black Basta's nasty tactics: Attack, assist, attack". Accesat în data de 04.04.2025, https://blog.barracuda.com/2024/05/18/black-basta-nasty-tactics

2. BlueVoyant. 2022. "Report CONTI Leaks 2022". Accesat în data de 04.04.2025, https://www.spirityenterprise.com/_files/ugd/f107e9_14108ba1522c4144b78f6672a598ebde.pdf?index=true

3. CIVILNET. 2024. „Ինչպես ԱՄՆ-ի կողմից հետախուզվող ՌԴ քաղաքացին փախավ Հայաստանի դատարանից". Accesat în data de 26.04.2025, https://www.civilnet.am/news/800556/%D5%AB%D5%B6%D5%B9%D5%BA%D5%A5%D5%BD-%D5%A1%D5%B4%D5%B6-%D5%AB-%D5%AF%D5%B8%D5%B2%D5%B4%D5%AB%D6%81-%D5%B0%D5%A5%D5%BF%D5%A1%D5%AD%D5%B8%D6%82%D5%A6%D5%BE%D5%B8%D5%B2-%D5%BC%D5%A4-%D6%84%D5%A1%D5%B2%D5%A1%D6%84%D5%A1%D6%81%D5%AB%D5%B6-%D6%83%D5%A1%D5%AD%D5%A1%D5%BE-%D5%B0%D5%A1%D5%B5%D5%A1%D5%BD%D5%BF%D5%A1%D5%B6%D5%AB-%D5%A4%D5%A1%D5%BF%D5%A1%D6%80%D5%A1%D5%B6%D5%AB%D6%81/

4. CSO. 2020. „TrickBot explained: A multi-purpose crimeware tool that haunted businesses for years". Accesat în data de 13.04.2025, https://www.csoonline.com/article/570169/trickbot-explained-a-multi-purpose-crimeware-tool-that-haunted-businesses-for-years.html

5. CSO. 2021. „Zero days explained: How unknown vulnerabilities become gateways for attackers". Accesat în data de 26.04.2025, https://www.csoonline.com/article/565704/zero-days-explained-how-unknown-vulnerabilities-become-gateways-for-attackers.html

6. CSO. 2022. „Conti ransomware explained: What you need to know about this aggressive criminal group". Accesat în data de 26.03.2025, https://www.csoonline.com/article/571503/conti-ransomware-explained-and-why-its-one-of-the-most-aggressive-criminal-groups.html

7. Cyberly. „What is Conti ransomware, and how does it work?". Accesat în data de 26.03.2025, https://www.cyberly.org/en/what-is-conti-ransomware-and-how-does-it-work/index.html

8. Dark Covenant. 2023. "Connections Between the Russian State and Criminal Actors". Accesat în data de 29.01.2025, https://www.recordedfuture.com/research/russian-state-connections-criminal-actors

9. EMSISOFT. 2025. „The State of Ransomware in Q1 2025". Accesat în data de 25.03.2025, https://www.emsisoft.com/en/blog/46626/the-state-of-ransomware-in-q1-2025/?utm_source=chatgpt.com

10. ESentire. 2025. „Initial Takeaways from the Black Basta Chat Leaks". Accesat în data de 28.04.2025, https://www.esentire.com/blog/initial-takeaways-from-the-black-basta-chat-leaks

11. Firts. 2025. „Black Basta Ransomware Leak: Key Findings and Insights". Accesat în data de 28.04.2025, https://www.first.org/blog/20250321-black-basta-ransomware-leak

12. Flare. 2025. "Deciphering Black Basta's Infrastructure from the Chat Leak". Accesat în data de 23.03.2025, https://flare.io/learn/resources/blog/deciphering-black-bastas-infrastructure-from-the-chat-leak/

13. FORESCOUT. 2022. „Analysis of Conti Leaks".Accesat în data de 11.04.2025, https://www.forescout.com/resources/analysis-of-conti-leaks/

14. Heimdal. 2024. „All about Conti Ransomware. From $180 Million Yearly Revenue to Internal Data Leakage". Accesat în data de 09.04.2025, https://heimdalsecurity.com/blog/what-is-conti-ransomware/

15. Intel471. 2025. „An in-depth look at Black Basta's TTPs". Accesat în data de 23.03.2025, https://intel471.com/blog/an-in-depth-look-at-black-bastas-ttps

16. Intel471. 2025. „Black Basta exposed: A look at a cybercrime data leaks". Accesat în data de 27.04.2025, https://intel471.com/blog/black-basta-exposed-a-look-at-a-cybercrime-data-leak

17. Kela. 2022. „Analysis of leaked Conti's Internal Data".Accesat în data de 11.04.2025, https://www.kelacyber.com/wp-content/uploads/2022/03/KELA-Intelligence-Report-ContiLeaks-1.pdf

18. Kela. 2025. „Inside the Black Basta Leak: How Ransomware Operators Gain Access". Accesat în data de 07.04.2025, https://info.ke-la.com/hubfs/Reports/KELA%20Report%20-%20Black%20Basta%20Leak_%20How%20Ransomware%20Operators%20Gain%20Access.pdf

19. PRODAFT. 2022. „CONTI Ransomware Group: In-depth Analysis". Accesat în data de 07.04.2025, https://resources.prodaft.com/conti-ransomware-group-report

20. ProofPoint, 2024, "Cyber Crime". Accesat în data de 29.01.2025, https://www.proofpoint.com/uk/threat-reference/cyber-crime

21. Qntinue. "Inside BlackBasta: What Leaked Conversations Reveal About Their Ransomware Operations". Accesat în data de 23.03.2025, https://www.ontinue.com/resource/inside-black-basta-leaked-coversations/

22. Rapid7. 2025. „2025 Ransomware: Business as Usual, Business is Booming". Accesat în data de 24.03.2025, https://www.rapid7.com/blog/post/2025/04/08/2025-ransomware-business-as-usual-business-is-booming/?utm_source=chatgpt.com

23. SentinelOne. „Black Basta". Accesat în data de 05.04.2025, https://www.sentinelone.com/anthology/black-basta/

24. SRM. 2025. „Cyber briefing note | The Black Basta leaks". Accesat în data de 08.04.2025, https://www.s-rminform.com/latest-thinking/the-blackbasta-leaks-cyber-briefing-note

25. TheSecMaster. 2025. „Black Basta Ransomware". Accesat în data de 30.03.2025, https://thesecmaster.com/blog/black-basta-ransomware

26. Trellix. 2022. „Conti Leaks: Examining the Panama Papers of Ransomware". Accesat în data de 10.04.2025, https://www.trellix.com/blogs/research/conti-leaks-examining-the-panama-papers-of-ransomware/

27. Trellix. 2025. „Analysis of Black Basta Ransomware Chat Leaks". Accesat în data de 27.04.2025, https://www.trellix.com/blogs/research/analysis-of-black-basta-ransomware-chat-leaks/

28. TrendMicro. 2022. „Black Basta". Accesat în data de 23.03.2025, https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta

Aceasta este al patrulea volum de proceedings al Conferinței Științifice Intelligence și Cultura de Securitate (ICS), care cuprinde lucrările prezentate în cadrul ediției din 2025 - ICS 2025, publicat de Academia Națională de Informații „Mihai Viteazul" (ANIMV). ICS continuă să ofere studenților o platformă pentru dialog academic și pentru a împărtăși realizările lor științifice.

Ediția actuală își extinde participarea la un spectru mai larg de contributori, incluzând atât doctoranzi, cât și studenți din programele de master, cu un interes crescut pentru domenii precum intelligence, securitate națională, istorie și relații internaționale.

Organizarea conferinței a fost posibilă datorită eforturilor continue ale doctoranzilor și ale conducătorilor de doctorat din cadrul Școlii Doctorale Intelligence și Securitate a ANIMV.

Anticipăm cu entuziasm noi discuții și schimburi de idei în viitoarea ediție a conferinței.

EDITURA ANIMV

ISSN 2972-1350
ISSN-L 2971-8139