INTELLIGENCE ŞI CULTURA DE SECURITATE

CONFERINȚA ȘTIINȚIFICĂ STUDENȚEASCĂ

PROCEEDINGS

VOLUMUL 2
2023

Editura Academiei Naţionale de Informaţii „Mihai Viteazul”

MODIFICAREA PEISAJULUI AMENINȚĂRILOR CIBERNETICE DATORITĂ IMPLICĂRII GRUPĂRILOR DE CYBERCRIME ÎN RĂZBOIUL RUSO-UCRAINEAN

Claudia-Alecsandra GABRIAN[*]

Abstract:

A year after the start of the Russia-Ukraine war, the threat landscape influenced by cybercrime groups has seen further changes, and while some groups have declared allegiance to the Russian government, others have split over ideological differences or remained apolitical, opting to capitalize on geopolitical instability for financial gain. Affiliates of these cybercrime groups are actively involved in operations targeting entities and critical infrastructures of Ukraine, as well as countries that have declared their support for Ukraine, posing a threat to supporting states.

This paper aims to highlight how financially motivated cybercrime actors capitalize on geopolitical instability and how they aid and abet Russian state interests, either by accident or on purpose. The objectives of the paper are to identify those cybercrime groups that use the ransomware attack or advanced persistent threat methods to carry out major cyber-attacks and how they changed their attack method after the outbreak of the conflict. The research methods used are qualitative, through document analysis and netnography, and the interpretation of the results is a justification of the involvement of cybercrime groups in this war. Netnography is used to analyse how these cybercrime groups discuss on public forums and groups, such as on Telegram, where they share all the information between members.

In the NIS Directive are mentioned 7 sectors of economic activity that should be insured a common high level of security of networks and IT systems. In the main results of this research, we identify that cybercriminals groups attack all these main sectors, such as energy, transport, banking, infrastructures, health, and digital infrastructures. There were identified changes in malware-as-a-service and ransomware-as-a-service attacks, as well as changes in cybercriminal tactics and methods to orchestrate an attack. Also, when we refer to ransomware, LockBit, and CL0P groups are currently the most important cybercrime groups that carry out major cyber-attacks on countries from Europe. The information used in the research comes from open sources, mainly oriented toward those originating from the Russian language and those found in the public groups of the affiliates of these groups.

Keywords: *cyber-attacks, cybercrime groups, cyber threats, ransomware, Telegram.*

[*] Student doctorand, Facultatea de Istorie și Filosofie, Universitatea Babeș Bolyai, domeniul de expertiză este relații internaționale și studii de securitate, date de contact: claudiaalecsandra@yahoo.com

Introducere

Transformarea digitală a condus la apariția de noi amenințări în spațiul cibernetic, iar războiul dintre Rusia și Ucraina a reprezentat un facilitator pentru grupările de criminalitate cibernetică, pentru a lansa noi tipuri de atacuri și pentru a obține câștiguri financiare, de pe urma acestui conflict. La începutul războiului, unii actorii sponsorizați de stat acționau în numele serviciilor din cadrul guvernului rus, iar unele grupări de *ransomware-as-a-service* (RaaS), motivate financiar, lucrau sub protecția guvernului rus și ulterior, și-au declarat public loialitatea pentru acesta. Aceste grupări s-au împărțit în tabere de susținere a beligeranților și s-au alăturat unor campanii masive de atacuri cibernetice, asupra țărilor care au sprijinit Ucraina.

Din 2022 și până în prezent, atacurile *ransomware* au continuat să reprezinte principalele amenințări cibernetice, care au crescut atât în intensitate, cât și prin câștigurile financiare obținute. Grupările de criminalitate cibernetică folosesc platforma Telegram drept un instrument cheie de comunicare, pentru a discuta despre viitoare atacuri cibernetice, prin crearea unor grupuri, din care fac parte persoane care se aliniază intereselor și obiectivelor lor.

Lucrarea prezintă o perspectivă asupra modificării peisajului amenințărilor cibernetice, care include studiul grupărilor de *cybercrime* și modul în care acestea sunt implicate în conflict, dar și rolul pe care îl are Federația Rusă, în lansarea de atacuri cibernetice. De asemenea, în cadrul lucrării vor fi prezentate date, care să justifice impactul pe care grupările de *cybercrime* l-au avut asupra operatorilor de servicii esențiale.

Scopul cercetării este de a evidenția modul în care, grupările de *cybercrime* și-au schimbat modul de operare și au realizat atacuri cibernetice, orientate asupra companiilor și organizațiilor din Europa. Obiectivele cercetării sunt: 1) identificarea grupărilor implicate în acest conflict; 2) evidențierea motivației acestora, în realizarea de atacuri de tip *ransomware* în contextul războiului. Întrebarea de cercetare este următoarea: Cum a influențat războiul dintre Rusia și Ucraina strategia grupărilor de criminalitate cibernetică, cu privire la selectarea viitoarelor victime?

Din punct de vedere metodologic, a fost utilizată analiza documentară, având la bază date statistice și rapoarte de la instituții (EUROPOL, CISA, Consiliul Uniunii Europene, FBI) și de la companii (Microsoft, Kaspersky, TrendMicro, IBM, SOCRadar), având ca temă criminalitatea cibernetică, iar documentele analizate conțin informații,

care evidenţiază modul în care aceste grupări de criminalitate cibernetică operează, cât şi traiectoria pe care o au, cu privire la modificarea strategiei lor de atac. O altă metodă folosită este netnografia, pentru analizarea discuţiilor de pe platforma de comunicare Telegram. Pe această platformă sunt regăsite grupuri şi canale, unde membrii grupărilor de *cybercrime* discută metode de atac, postează foarte detaliat atacurile pe care le realizează şi fac referire la datele pe care le obţin. Utilizarea netnografiei este relevantă în acest context, deoarece grupările de *cybercrime* şi-au transferat activitatea de pe *dark web*, pe canelele de Telegram, care în momentul actual este considerat un instrument specializat în criminalitatea cibernetică.

Principala limită a cercetării este legată de fluxul mare de informaţii regăsite pe canalele de Telegram, fiind necesară verificarea acestora, din surse alternative, pentru a evita riscul dezinformării. O altă limită este legată de literatura academică de specialitate, având în vedere, că există un număr limitat de lucrări pe subiectul cercetat.

Cybercrime

Potrivit unui raport Kaspersky, criminalitatea cibernetică reprezintă o activitate desfăşurată în mediul online, unde majoritatea celor care întreprind astfel de acţiuni sunt criminali cibernetici sau hackeri, care vizează sau folosesc un computer, o reţea de computere sau un dispozitiv în reţea, pentru a obţine câştiguri financiare, în urma atacurilor cibernetice pe care le realizează (Kaspersky, 2019a).

Criminalii cibernetici sunt persoane sau grupuri care utilizează programe *malware* şi alte tipuri de *software*, pentru a realiza activităţi rău intenţionate asupra anumitor sisteme sau reţele digitale, având scopul de a fura informaţii sensibile ale companiilor, care conţin chiar şi datele personale ale indivizilor, de pe urma cărora, să obţină profit. Criminalii cibernetici accesează pieţele subterane, cum ar fi cele de pe *dark web*, pentru a tranzacţiona bunuri şi servicii rău intenţionate, cum ar fi instrumente de hacking sau date furate (Trend Micro, 2019).

Cel mai important act legislativ referitor la criminalitatea cibernetică este Convenţia de la Budapesta, care reprezintă şi primul tratat internaţional, prin care sunt incriminate infracţiunile comise în mediul online. Importanţa acestuia reiese din faptul că, cele mai relevante state în domeniul securităţii cibernetice sunt semnatare a acestuia. În prezent, sunt 68 de semnatari ai acestei convenţii, state din UE şi NATO, 21 de state au semnat sau urmează să adere, iar Ucraina este unul dintre aceşti semnatari. Obiectivul principal este de a urmări o

politică penală comună, care vizează protecţia societăţii împotriva criminalităţii informatice, în special prin adoptarea unei legislaţii adecvate şi încurajarea cooperării internaţionale (Council of Europe, 2014).

În februarie 2022, când a început conflictul dinte Federaţia Rusă şi Ucraina, grupările de cybercrime erau active în spaţiul cibernetic, derulând activităţi, precum vânzarea de date, obţinute ca urmare a derulării de atacuri cibernetice tip *ransomware.* Ascensiunea platformei Telegram a fost observată începând de atunci, deoarece au fost create grupuri unde se discutau detalii despre război şi despre atacurile cibernetice realizate, în context, fiind relevante următoarele grupuri: *Donbass Devushka* (transcris din limba rusă), *Ria Novosti* (transcris din limba rusă), *POKOT* (transcris din limba rusă). Analizând discuţiile din cadrul acestor grupuri, am observat că, infractorii cibernetici au coordonat atacuri cibernetice împotriva adversarilor de pe această platformă, unde au şi postat date cu privire la atacurile cibernetice realizate.

Răspândirea grupărilor de *cybercrime* în mediul digital a facilitat promovarea mesajelor de susţinere a acestora, iar cel mai relevant exemplu este gruparea de *ransomware Conti*. Aceasta şi-a promovat sprijinul pentru armata rusă şi administraţia rusă, enunţând faptul că, „dacă cineva va organiza un atac cibernetic sau orice altă activitate împotriva Rusiei, vor folosi toate resursele disponibile pentru a ataca infrastructurile critice ale unui inamic" (Bleih Adi, 2023). Gruparea CONTI este un exemplu menţionat în această secţiune, deoarece a fost una dintre cele mai active grupări de ransomware până în primăvara lui 2022, când a fost desfiinţată. Datorită legăturii confirmate a acesteia cu guvernul rus, a cunoscut schimbări semnificative la nivel organizaţional, care ulterior, au dus la scurgeri mari de date interne şi ulterior, la închiderea definitivă a serverelor acesteia pe serverul TOR (Warminsky Joe, 2022)

Peisajul ameninţărilor a fost modificat de către grupările de *cybercrime*, deoarece acestea şi-au schimbat modul de atac, în contextul războiului dintre Rusia şi Ucraina şi s-a creat o divizare în rândul acestor grupări, unele au fost în tabăra pro-rusă, iar altele în cea pro-ucraineană. Grupările care au continuat colaborarea cu guvernul rus au fost susţinute atât direct, cât şi indirect, iar cele care şi-au recunoscut loialitatea faţă de guvern, au primit şi mai mult sprijin pentru a se implica activ în operaţiuni care vizau derularea de atacuri cibernetice asupra

infrastructurii critice a Ucrainei şi a ţărilor care şi-au oferit sprijinul pentru Ucraina (Insikt Group, 2023).

Grupările de cybercrime

Grupările de *cybercrime* îşi concentrează atacurile asupra acelor sectoare şi organizaţii care reprezintă pentru ei ţinte uşoare şi despre care ei cred, că vor genera cel mai mare flux de date. Aceste grupări folosesc ofertele lor de atac drept un serviciu pentru alte grupări de criminalitate cibernetică, care pot ajuta la creşterea numărului de atacuri cibernetice (Steer Jason, 2023).

Atacul de tip *ransomware* reprezintă un *malware*, care împiedică sau limitează utilizatorii să-şi acceseze sistemul, prin criptarea fişierelor utilizatorilor până când se plăteşte o răscumpărare (Microsoft, n.d.). Există două categorii principale de ransomware: *ransomware locker* şi *crypto ransomware*. R*ansomware locker* afectează funcţiile de bază ale computerului, iar *crypto ransomware* afectează doar anumite fişiere care sunt criptate, iar pentru reobţinerea datelor, membrii grupărilor de *cybercrime* solicită o răscumpărare, pentru a transmite o cheie de decriptare (Trend Micro, 2011). Primele atacuri de ransomware moderne au fost raportate în Rusia, în 2005, iar din acel moment, acest tip de atac cibernetic a fost răspândit şi în exteriorul teritoriului, unde au fost dezvoltate din ce în ce mai multe tipuri. La momentul actual reprezintă cele mai avantajoase tipuri de atacuri cibernetice, datorită câştigurilor obţinute. (Kaspersky, 2019b)

Din punctul de vedere al analizării grupărilor de *cybercrime* după modelul de atac *ransomware*, acestea se evidenţiază în fiecare lună, prin numărul de atacuri pe care le realizează asupra anumitor sectoare şi ţări, astfel, fiind identificate 5 grupări de *ransomware*, care sunt top 5 în acest moment: *LockBit*, *CL0P*, *BlackCat*, *Royal* şi *BlackBasta* (SOCRadar, 2023a). În continuare vom analiza activitatea grupărilor LockBit şi CL0P.

De la începutul războiului dintre Rusia şi Ucraina, gruparea LockBit este responsabilă pentru peste o treime din toate atacurile *ransomware*, din a doua jumătate a anului precedent şi până în prezent (SOCRadar, 2023b). Prezenţa grupării LockBit a fost identificată pentru prima dată, în septembrie 2019 şi a devenit cel mai activ grup de ransomware, din 2022 şi până acum, aspect facilitat şi de destructurarea grupării Conti, în primăvara lui 2022. Din punct de vedere financiar, pierderile cauzate companiilor care au fost ţintele acestei grupări pot ajunge până la miliarde de dolari (SOCRadar, 2023c).

În prezent, gruparea LockBit rulează o versiune actualizată a malware-ului din 2022, care se numește LockBit Black sau LockBit 3.0. Gruparea se bazează pe o abordare bazată pe afiliați, iar aceștia vizează companii și organizații din aria operatorilor de servicii esențiale. LockBit își realizează propria promovare pe forumurile de criminalitate cibernetică, prin anunțuri de recrutare și concursuri, iar aceste inițiative atrag numeroși afiliați (SOCRadar, 2023d).

Această grupare respectă un tipar identificat și la alte grupări de criminalitate cibernetică, folosind limba rusă pentru a realiza atacuri, sistemele vizate fiind infectate doar dacă, limba sistemului de operare nu este cea rusă sau orice altă limbă înrudită cu rusa sau cu limbile oficiale ale statelor aliate Federației Ruse, spre exemplu araba (Siria) și tătara (Rusia) (SOCRadar, 2023e). De asemenea, în anumite situații este folosită identificarea locației, prin utilizarea adresei IP, iar dacă țara de origine nu se potrivește cu niciuna dintre țările specificate de atacatori, în codul sursă al *malware*-ului, atacul cibernetic trece la etapa următoare de infectare. Deși, acest grup de ransomware susține că nu se implică în politică, multe dintre țintele sale sunt țările aliate NATO și Ucrainei (SOCRadar, 2023f). Potrivit raportului realizat de către DarkFeed, până în acest moment, LockBit a realizat în total 1875 de atacuri, 740 de atacuri au avut loc în 2022, iar 548 în 2023 (DarkFeed, 2023a). Ceea ce se poate evidenția este faptul că, atacurile acestei grupări sunt în continuă creștere, iar menținerea frecvenței actuale a acestora poate genera depășirea numărului din 2022, pentru anul 2023.

Interviurile realizate cu membrii acestor grupări sunt rare, iar un interviu relevant este al scriitorul Dmitry Smilyanets, din cadrul *Recorded Future*. Acesta i-a adresat întrebări unui membru din gruparea LockBit, pentru a obține informații cu privire la metoda de atac a acestei grupări. Acest membru menționează că, din perspectiva lor, nu contează atât de mult criptarea datelor, cât importanța informațiilor criptate, deoarece pentru nedezvăluirea acestora, compania va plăti mai mult decât pentru decriptarea lor (Smilyanets Dmitry, 2021a). Un alt aspect important este legat de faptul că, membrii grupării sunt încrezători în sistemul propriu de securitate, însă, pentru a avea un back-up, au realizat mai multe copii de siguranță ale datelor criptate pe mai multe servere din diferite părți ale lumii, precum și copii de rezervă separate fizic de Internet (Smilyanets Dmitry, 2021b). Din 2021, afiliații grupări LockBit folosesc *dubla extorcare*, care se referă la criptarea datelor victimelor combinată cu exfiltrarea acelor date și solicitarea unei răscumpărări pentru nu fi publicate (CISA, 2023). Potrivit unui raport IBM, în anul

2022, extorcarea a reprezentat principala abordare asociată atacului tip *ransomware*. Europa a fost cea mai vizată regiune, reprezentând 44% din cazurile de extorcare observate, deoarece infractorii cibernetici au exploatat tensiunile geopolitice (IBM, 2023a).

Infractorii cibernetici vizează adesea cele mai vulnerabile industrii, întreprinderi şi regiuni. Spre exemplu, industria manufacturieră a fost cea mai extorcată în 2022 şi a fost cea mai atacată industrie pentru al doilea an consecutiv (IBM, 2023b). Industria manufacturieră reprezintă o ţinţă pentru aceste grupări, deoarece acestea deţin proprietate intelectuală, iar datele acestea sunt valoroase pentru aceştia, iar dat fiind faptul că, scopul lor principal este producţia şi livrarea în timp a produselor, îi determină să plătească răscumpărarea, pentru a nu exista întreruperi (Exalens, 2022). De la începutul anului 2022, au fost folosite instrumente şi tehnici care să ajute atacatorii de ransomware, să evolueze şi să lanseze atacuri asupra operatorilor de servicii esenţiale, ceea ce a dus la o creştere de 63,2% a grupărilor de ransomware, în primul trimestru al anului 2022. Peste 50 de grupări de ransomware au vizat şi compromis peste 1.200 de organizaţii, în prima jumătate a anului 2022 (TRENDMicro, 2023).

Gruparea CL0P a fost identificată pentru prima dată, la începutul anului 2019 şi este asociată cu gruparea TA505, conform MITRE ATT&CK Framework. TA505 este activ din 2014 şi este cunoscut pentru schimbarea frecventă a malware-ului şi pentru campaniile de ransomware, care implică funcţia CL0P (MITRE, n.d.). Această grupare deşi a început să fie activă din ianuarie 2022, doar în anul 2023 a realizat atacuri cibernetice, pe care le-a derulat asupra operatorilor de servicii esenţiale din Europa. La fel ca gruparea LockBit, atacurile cibernetice ale acestei grupări nu sunt executate la adresa sistemelor care utilizează limba rusă şi limbile înrudite sau cele ale statelor aliate Federaţiei Ruse (SentinelOne, n.d.).

Informaţiile relevante, pentru analizarea grupărilor LockBit şi CL0P au fost identificate pe grupurile de Telegram *SecurityLab.ru*, *Russian OSINT* şi *SecAtor*, unde s-au postat mai multe mesaje referitoare la atacurile realizate de acestea. Gruparea CL0P a atras atenţia prin faptul că, a realizat 70 de atacuri într-o săptămână, dintre care 42 într-o singură zi. Potrivit paginii Twitter *DarkFeed*, în luna martie, gruparea a realizat 98 de atacuri fiind clasificată pe cel de-al doilea loc, după LockBit, care a derulat 99 de atacuri (Twitter, Ido_cohen2 n.d.a). De asemenea, ultima statistică pentru luna iunie, publicată tot pe pagina Twitter *DarkFeed,* evidenţiază faptul că, gruparea CL0P ocupă primul loc în clasamentul

pentru cele mai multe atacuri realizate de grupările de ransomware, adică 89, iar gruparea LockBit ocupă locul 2, cu doar 67 de atacuri (Twitter, Ido_cohen2 n.d.b). De asemenea, potrivit unei analize *DarkFeed*, gruparea CL0P a realizat până în prezent 393 de atacuri, dintre care, doar 19 atacuri în anul 2022, iar de la începutul anului 2023 și până în prezent a realizat 247 de atacuri, ceea ce reprezintă o creștere exponențială a activității acestei grupări (DarkFeed, 2023b). Aceste rezultate sunt importante pentru a justifica faptul că, grupările de ransomware sunt foarte active și pentru a prezenta faptul, că realizează din ce în ce mai multe atacuri cibernetice. Dat fiind faptul că, aceste date sunt postate în timp real, ajută la monitorizarea acestor grupări și la observarea tendințelor pe care le au în fiecare lună, cu impact major în anumite zile, de asemenea, aceste date justifică selectarea acestor două grupări pentru subiectul cercetat.

Cea mai mare atenție asupra grupării CL0P a fost alocată în urma celui mai recent și important atac cibernetic realizat de aceasta, care a fost derulat prin exploatarea vulnerabilităților instrumentului de transfer fișiere MOVEit, care este folosit la nivelul mediului privat, pentru a partaja fișiere. Acesta a determinat, ca sute de companii să fie compromise, fiindu-le criptate date sensibile, iar gruparea a luat legătura direct cu ele pentru a discuta ei înșiși despre răscumpărare. În urma analizării atacului de către CISA, aceștia au fost prezenți încă din 2021, în sistemul MOVEit, au testat metode de atac de mai multe ori pe parcursul a doi ani, realizând atacurile efective în perioada sărbătorilor (CISA, 2023). Prin această abordare, atacatorii au exploatat vulnerabilitatea umană a potențialelor victime, acestea acordând atenție redusă tentativelor de manipulare în perioadele festive ale anului (Abrams Lawrence, 2023).

Potrivit unui raport al companiei de securitate cibernetică Thales, pe tema războiului dintre Rusia și Ucraina, sunt prezentate date care justifică faptul că, la începutul conflictului majoritatea atacurilor au afectat doar Ucraina. A fost identificată o tendință începând cu vara anului 2022, deoarece în țările europene au avut loc aproape la fel de multe atacuri cibernetice, câte au fost în Ucraina până în acel moment. Pentru anul 2023, în primul trimestru, majoritatea atacurilor au avut loc în interiorul Uniunii Europene. Cele mai importante sectoare afectate au fost administrația publică europeană, sectorul financiar, sectorul transporturilor, sectorul comunicațiilor electronice, sectorul energetic, sectorul sănătății și sectorul educației (THALES, 2023).

Guvernul rus şi ameninţările cibernetice

Actualul război se desfăşoară cu implicarea grupărilor de *cybercrime,* inclusiv cele aliniate intereselor strategice ale Federaţiei Ruse, ceea ce denotă, că tehnologia cibernetică poate să fie utilizată concomitent cu operaţiunile militare. Un exemplu este cel al evenimentelor din 2014, când Rusia a invadat Crimeea, iar Ucraina a fost victima unor atacuri cibernetice semnificative[1]. În Rusia sunt prezente grupări sponsorizate de guvern, care pot să îşi folosească capabilităţile cibernetice pentru a lansa atacuri majore, deoarece primesc protecţie în schimbul oferirii serviciilor lor guvernului, fiind susţinute să realizeze operaţiuni cibernetice la scară largă, astfel, atacuri asupra Ucrainei sunt justificate de către aceste grupări, deoarece acţionează în numele statului rus, pentru a obţine avantaje strategice sau financiare. (Górka, 2022).

Serviciile secrete ruse sunt cunoscute pentru implicarea lor în realizarea de atacuri cibernetice de tip *Advanced Persistent Threat* (APT), orientate către ţinte de nivel înalt, cum ar fi statele şi marile corporaţii, cu scopul de a fura informaţii sensibile, pe o perioadă lungă de timp (Kaspersky 2020). Grupările APT sponsorizate de guvernul rus folosesc capabilităţi cibernetice avansate şi vizează, în special, infrastructura critică a adversarilor, menţinându-şi prezenta uneori nedetectabilă în mediile ţintă. Toată activitatea este coordonată de serviciile ruse de informaţii, pentru a se asigura că toate cerinţele sunt îndeplinite, iar în prezent sunt dezvoltate capabilităţi cibernetice, care să răspundă obiectivelor de politică internă şi externă pe care guvernul rus le are (Rosengren, 2023a).

Implicarea serviciilor secrete ruse în realizarea de atacuri cibernetice conexate cu grupările pe care le susţin, a fost pregătită înaintea începerii războiului în 2022, deoarece un grup afiliat statului rus, sub numele de Nobelium sau APT29*,* recunoscut pentru relaţia cu Serviciul Rus de Informaţii Externe (SVR), a fost identificat încă din luna mai a anului 2021, în realizarea de atacuri care au vizat Ucraina. Obiectivele acestei grupări sunt compromiterea sistemelor şi serviciilor ucrainene de comunicaţii, transport, energie şi apărare (Schulze Matthias, 2023.a). Potrivit The Record, Nobelium este recunoscut pentru acţiuni de spionaj asupra entităţilor diplomatice ale ţărilor care fac parte

[1] Se pot menţiona atacuri DDoS asupra reţelelor de comunicaţii ucrainene, iar grupurile pro-ruse au realizat o serie de atacuri cibernetice, pentru a manipula alegerile prezidenţiale din Ucraina.

din NATO și UE („Grupul de hacking susținut de Kremlin pune un accent nou pe furtul de acreditări", n.d.).

Pe 23 februarie 2022, Agenția Rusă de Informații Militare (GRU) a lansat mai multe atacuri cibernetice, prin gruparea APT28, care au avut drept obiectiv ștergerea datelor pe care guvernul ucrainean le avea despre război. Acest tip de atac este un exemplu, pentru a justifica interesul Federației Ruse de a utiliza atacuri cibernetice, care să reprezinte pentru ei un avantaj tactic (Schulze Matthias. 2023.b). De asemenea, atacul Rusiei, din 24 februarie 2022, asupra sistemului de comunicații prin satelit Viasat, a avut drept scop oprirea comunicațiilor prin satelit între Ucraina și Europa, însă, acest atac nu le-a oferit un avantaj operațional, deoarece nu a reușit să împiedice operațiunile de comandă și control ucrainene (Schulze Matthias. 2023.c).

Pe grupul de Telegram *Russian OSINT* s-au postat informații, cu privire la modul în care Federația Rusă se raportează la spațiul cibernetic. În Federația Rusă sunt necesare noi abordări, care să fie adaptate la schimbările tehnologice, iar astfel, guvernul rus a reconfigurat modul de raportare la controlul și supravegherea spațiului cibernetic. Din punct de vedere legislativ, Rusia a refuzat să semneze Convenția de la Budapesta, însă, face în momentul actual schimbări legislative și normative, cu privire la modul de raportare la atacurile cibernetice și modul în care, fondurile criminalilor cibernetici pot să fie utilizate. Federația Rusă oferă noi oportunități, pentru actorii sprijiniți de stat, pentru lansarea de atacuri cibernetice și pentru accesarea ilegală a sistemelor statelor (Gritsenko et al., 2020).

Cu toate acestea, chiar dacă Rusia are capacități de a ataca diverse ținte în mediul online, nu au fost identificate operațiuni cibernetice ofensive, care să ofere Federației Ruse avantajul strategic pe câmpul de luptă, observându-se chiar o limitare a acestora. O operațiune cibernetică necoordonată cu alte operațiuni cibernetice, nu este suficientă pentru a obține avantaje strategice pe terenul de luptă. Astfel, sunt necesare atacuri cibernetice de mai multe tipuri, care să fie realizate concomitent, pentru a bloca sisteme ale anumitor instituții sau organizații de importanță strategică. Grupările APT reprezintă o amenințare în continuă dezvoltare la nivel global, printre cele mai importante obiective regăsindu-se spionajul, dezinformarea și sabotajul cibernetic. Motivația strategică a Federației Ruse este evidențierea puterii și catalogarea țării drept o super putere cibernetică (Rosengren, 2023b).

Potrivit Statista, în ultimii ani, rușii s-au confruntat cu un număr tot mai mare de amenințări cibernetice, cum ar fi breșe de securitate,

atacuri malware şi frauda digitală (Statista, 2023). Cele mai multe breşe de securitate din ţară au implicat pierderi de date personale, cum ar fi nume, e-mailuri sau adrese, ceea ce denotă faptul că, şi Federaţia Rusă a fost atacată de către grupările pro-ucrainene (Lewis James Andrew, 2022a).

În Rusia sunt regăsite cele mai avansate grupări de criminali cibernetici din lume, pe care guvernul rus le protejează, le oferă imunitate, însă, câştigurile sunt folosite în avantajul statului rus. Regulile după care se ghidează membrii acestor grupări sunt simple, aceştia nu au permisiunea să atace site-urile ruseşti, nu trebuie să compromită confidenţialitatea legăturii cu serviciile de informaţii ruse şi trebuie să împartă ceea ce câştigă. Unele dintre grupările de ransomware active au echipe specializate, care sunt împărţite în funcţie de sarcina pe care trebuie să o realizeze, fiecare sarcină fiind specifică cu metoda de atac şi cu selectarea victimei (Lewis James Andrew, 2022b).

Concluzii

Ransomware-ul este utilizat de către grupările de cybercrime, pentru a exploata victimele şi a devenit o constantă în rândul ameninţărilor cibernetice, mai ales prin metoda dublei extorcări. Atacurile, care au fost realizate în urma izbucnirii conflictului dintre Rusia şi Ucraina, au vizat şi operatorii de servicii esenţiale din Europa, iar infractorii cibernetici şi-au dezvoltat noi tipuri de atac, pentru a indisponibiliza accesul la date. Având în vedere elementele prezentate, putem concluziona că, fenomenul criminalităţii cibernetice nu a fost afectat de către război, ci a fost potenţat, date fiind dezvoltarea tehnologică a acestora şi amploarea atacurilor derulate.

Prin cercetarea realizată am răspuns la întrebarea de cercetare, deoarece am identificat grupările LockBit şi CL0P drept cele mai active grupări de ransomware. Aceste grupări şi-au orientat atenţia înspre ţări care sprijină Ucraina, iar divizarea acestor grupări în două tabere, nu face altceva decât să demonstreze faptul că, strategia lor de atac şi modul în care acţionează, au fost influenţate de către acest război, iar grupările şi-au dezvoltat tehnica de atac. De asemenea, implicarea guvernului rus în atacuri cibernetice asupra Ucrainei, este justificată prin grupările APT, care sunt sponsorizate de către serviciile secrete, din cadrul guvernului rus. Motivaţia acestor grupări fiind de natură strategică şi financiară, în scopul perturbării în primul rând, al sistemelor de importanţă strategică a Ucrainei şi a ţărilor din Uniunea Europeană. Aceste aspecte ne-au permis atingerea obiectivelor de cercetare. Grupările de cybercrime au o

prezenţă constantă în mediul online şi se constată faptul că, acestea au folosit platforma Telegram drept un instrument cheie de comunicare între ei şi adepţii grupărilor, pentru a conduce operaţiuni care să se alinieze intereselor şi obiectivelor lor. Prin analiza documentară au fost identificate elementele specifice grupărilor de cybecrime, cum ar fi: tipologia lor, ţintele pe care le au şi modul de operare. De asemenea, documentele strategice identificate şi analizele statistice au reprezentat surse de documentare, bazate pe cercetări empirice relevante subiectului cercetat. Prin netnografie, s-au putut contura idei despre modul în care, grupările de cybercrime sunt prezente pe un canal public de socializare, cum este Telegram. Această sursă deschisă oferă o multitudine de perspective, cu privire la ceea ce se discută între membrii grupărilor, în limba lor nativă, cât şi evidenţierea modului în care, aceste grupări au făcut o tranziţie de la grupurile de pe dark web, pe o platformă unde oricine poate să aibă acces la conţinutul lor. Cu siguranţă, unele mesaje regăsite sunt criptate şi nu pot să fie citite doar de către cei care au cheia de decriptare, însă, acestea au fost puţine, comparativ cu datele publicate încă de la începutul războiului. Grupurile de Telegram menţionate în lucrare sunt active şi acum, pot să fie accesate de către oricine, iar mesajele transmise despre război şi atacurile cibernetice realizate sunt postate în fiecare zi, cu o medie de până la 1.000 de postări pe zi.

Direcţiile viitoare de cercetare propuse s-ar putea orienta înspre extinderea cercetării, o analiză a atacului de tip ransomware, pentru a se analiza dacă acesta va continua să reprezinte o ameninţare majoră, pentru ţările care au sprijint Ucraina şi în anul 2023. De asemenea, o analiză a modului în care, grupările de cybecrime vor rămâne active sau nu pe canelele de Telegram, cât şi modul în care, îşi vor coordona activităţile viitoare. Astfel, platforma Telegram ar putea să fie analizată din punct de vedere al atractivităţii, pentru grupările de cybercrime, în comparaţie cu reţeaua TOR sau din punct de vedere al modificării tipului de activitate la nivelul acesteia – ce se vehiculează la nivelul grupurilor, care încă sunt active şi dacă mesajele şi conţinutul postat pe aceste canale este schimbat sau nu. De asemenea, o altă direcţie de cercetare ar putea fi analiza cantitativă a atacurilor cibernetice asupra ţărilor care sprijină Ucraina, unul dintre nivelurile luate în considerare fiind cel al sectorului de proveniență al infrastructurii victimă.

Referințe bibliografice:

1. Abrams Lawrence. 2023. „*Clop ransomware claims responsibility for MOVEit extortion attacks*" BleepingComputer. Accesat la data de 19.04.2023 la https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-moveit-extortion-attacks/

2. Antoniuk Daryna. 2023. „*Kremlin-backed hacking group puts fresh emphasis on stealing credentials*" Therecord.media. Accesat la data de 07.05.2023 la https://therecord.media/nobelium-hacking-group-stealing-credentials

3. BleepingComputer. 2023. „*The Great Exodus to Telegram: A Tour of the New Cybercrime Underground*" Accesat la data de 11.07.2023 la https://www.bleepingcomputer.com/news/security/the-great-exodus-to-telegram-a-tour-of-the-new-cybercrime-underground/

4. Bleih Adi. Lerner Dov. 2023 „*How Telegram became the battlefront of the Russia-Ukraine cyberwar*" n.d. Cybersixgill. Accesat la data de 25.04.2023 la https://cybersixgill.com/news/articles/telegram-russia-ukraine-cyberwar.\

5. Braue David. 2023. "*How Geopolitics Affects Cybersecurity*". Cybercrime Magazine. Accesat la data de 20.04.2023 la https://cybersecurityventures.com/how-geopolitics-affects-cybersecurity/

6. CISA. 2023. "*#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 Vulnerability*" Accesat la data de 17.07.2023 la https://www.cisa.gov/sites/default/files/2023-07/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_8.pdf

7. CISA. 2023. "*CISA and Partners Release Joint Advisory on Understanding Ransomware Threat Actors: LockBit*" Accesat la data de 11.05.2023 la https://www.cisa.gov/news-events/alerts/2023/06/14/cisa-and-partners-release-joint-advisory-understanding-ransomware-threat-actors-lockbit

8. CISA. 2023. „*Understanding Ransomware Threat Actors: LockBit*" Accesat la data de 07.05.2023 la https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

9. CISA. n.d. „*Combatting Cyber Crime*". Accesat la data de 18.04.2023 la https://www.cisa.gov/combatting-cyber-crime

10. Council of Europe 2014. "*The Budapest Convention (ETS No. 185) and its Protocols*" Accesat la data de 14.05.2023 la https://www.coe.int/en/web/cybercrime/the-budapest-convention

11. DarkFeed. 2023 „*CLOP-Overview*" Accesat la data de 11.07.2023 la https://darkfeed.io/2023/04/27/clop-overview/

12. DarkFeed. 2023. „Lockbit-Overview". Accesat la data de 11.07.2023 la https://darkfeed.io/2023/04/27/lockbit-overview/

13. DNSC. n.d. "*Informații generale despre NIS*" Accesat la data de 13.07.203 la https://dnsc.ro/pagini/informatii-generale-despre-nis

14. Eurojust. n.d. „*Cybercrime*". Accesat la data de 18.04.2023 la https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime

15. Exalens. 2023. "*A Troubling Trend Continues: Why Manufacturing Remains the Top Target for Cyber Criminals*" Accesat la data de 17.07.2023 la https://www.exalens.com/post/a-troubling-trend-continues-why-manufacturing-remains-the-top-target-for-cyber-criminals

16. FBI. n.d. „*The cyber threat*" Accesat la data de 02.05.2023 la https://www.fbi.gov/investigate/cyber

17. Glover Claudia. 2023. „*Russia's invasion of Ukraine has changed cybercrime forever, says report*" Accesat la data de 16.05.2023 la https:// techmonitor.ai/technology/cybersecurity/how-russia-ukraine-war-changed-cybercrime

18. Górka Marek. 2022. „*A Definitional Framework for Cyber Warfare. The Ukrainian Aspect*" Polish Political Science Yearbook 51: 1–14. Accesat la data de 18.05.203 la https://doi.org/10.15804/ppsy202272

19. Gritsenko Daris. Kopotev, Mikhail. 2020. "*Digital Russia Studies: An Introduction*". The Palgrave Handbook of Digital Russia Studies. Accesat la data de 20.05.2023 la https://cris.maastrichtuniversity.nl/en/publications/digital-russia-studies-an-introduction

20. Huntley Shane. 2023. „*Fog of war: how the Ukraine conflict transformed the cyber threat landscape*". Google. Accesat la data de 19.05.2023 la https:// blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

21. IBM. 2023. „*IBM Report: Ransomware Persisted Despite Improved Detection in 2022*" Accesat la data de 12.07.2023 la https://newsroom. ibm.com/2023-02-22-IBM-Report-Ransomware-Persisted-Despite-Improved-Detection-in-2022

22. Insikt Group. 2023. *„Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine"*. Accesat la data de 16.07.2023 la https://www. recordedfuture.com/dark-covenant-2-cybercrime-russian-state-war-ukraine

23. Intel471. 2022. „*Why cybercriminals are flocking to Telegram*". Intel471. Accesat la data de 28.04.2023 la https://intel471.com/blog/why-cybercriminals-are-flocking-to-telegram

24. INTERPOL. d.d. „*Cybercrime*". Accesat la data de 18.04.2023 la https://www.interpol.int/Crimes/Cybercrime

25. Iyengar Rishi. 2023. „*How the Ukraine War Has Changed Russia's Cyberstrategy"* Accesat la data de 14.05.2023 la https://foreignpolicy.com/ 2023/02/24/russia-ukraine-war-cybercrime-strategy/

26. Kaspersky. 2019 "*What is Ransomware?*". Accesat la data de 15.04.2023 la https://www.kaspersky.com/resource-center/threats/ ransomware

27. Kaspersky. 2019. „*What is cybercrime? How to protect yourself from cybercrime*" Accesat la data de 16.04.2023 la https://www.kaspersky.com/ resource-center/threats/what-is-cybercrime

28. Kaspersky. 2020. „*What Is an Advanced Persistent Threat (APT)?*" Accesat la data de 12.07.2023. https://www.kaspersky.com/resource-center/ definitions/advanced-persistent-threats

29. KELA. 2023. „*Telegram: How a messenger turned into a cybercrime ecosystem by 2023*". Accesat la data de 10.05.2023 la https://ke-la.com/resource/telegram-how-a-messenger-turned-into-a-cybercrime-ecosystem-by-2023/

30. Lewis James Andrew. 2022. "*A Dangerous Moment for Russian Cybercrime May Get Worse*". Accesat la data de 11.07.2023 la https://www.barrons.com/articles/a-dangerous-moment-for-russian-cybercrime-may-get-worse-51644936090

31. Lewis James Andrew. 2022. "*Cyberwar and Ukraine*". CSIS. Accesat la data de 08.07.2023 la https://www.csis.org/analysis/cyber-war-and-ukraine

32. Martin Alexander. 2023. „*Ransomware group Clop issues extortion notice to 'hundreds' of victims*" Therecord.media. Accesat la data de 06.05.2023 la https://therecord.media/clop-extortion-hundreds-organizations-moveit-vulnerability

33. Microsoft. n.d. „*Ce este ransomware-ul?*" Accesat la data de 16.04.2023 la https://www.microsoft.com/ro-ro/security/business/security-101/what-is-ransomware

34. MITRE. n.d. „*TA505*". Accesat la data de 12.07.2023 la https://attack.mitre.org/groups/G0092/

35. Positive Technologies. 2022. "*Cybercriminal market in Telegram*". Accesat la data de 12.07.2023 la https://www.ptsecurity.com/ww-en/analytics/cybercriminal-market-in-telegram/

36. Rosengren Oscar. 2023. "*The Five Bears: Russia's Offensive Cyber Capabilities*" Accesat la data de 10.07.2023 la https://greydynamics.com/the-five-bears-russias-offensive-cyber-capabilities/

37. Schulze Matthias. 2023. "*Cyber Operations in Russia's War against Ukraine*". Accesat la data de 04.06.2023 la https://www.swp-berlin.org/10.18449/2023C23/

38. SentinelOne. n.d. "*CL0P*". Accesat pe 22.04.2023 la https://www.sentinelone.com/anthology/clop/

39. Smilyanets Dmitry. 2021. „*An interview with LockBit: The risk of being hacked ourselves is always present*" Therecord.media. Accesat pe 05.05.2023 la https://therecord.media/an-interview-with-lockbit-the-risk-of-being-hacked-ourselves-is-always-present

40. SOCRadar. 2023. „*Dark Web Profile: LockBit 3.0 Ransomware*" Accesat pe 27.04.2023 la https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/

41. Statista. 2023. "*Information security and cyber crime in Russia - statistics & facts*" Accesat pe 08.05.2023 la https://www.statista.com/topics/7335/informatica-securitatea-si-crima-cibernetica-in-russia/#topicOverview23

42. Steer Jason. 2023. „*More DDoS, More Leaks: Where Ransomware is Headed in 2023*" Infosecurity magazine. Accesat pe 12.07.2023 la https://www.infosecurity-magazine.com/blogs/ddos-leaks-ransomware-2023/

43. THALES. 2023. „*FROM UKRAINE TO THE WHOLE OF EUROPE: THE CYBER CONFLICT ENTERS A NEW STAGE*” 2023. Thales Group. Accesat pe 11.07.2023 la https://www.thalesgroup.com/ro/hwl-alalm/security/press_release/din-ucraina-nivelul-intregii-europe-conflictul-cibernetic-intra

44. TRENDMicro. 2011. “*Ransomware Definition*” Accesat pe 16.05.2023 la https://www.trendmicro.com/vinfo/us/security/definition/ransomware

45. TRENDMicro. 2023. „*5 Types of Cyber Crime Groups*”. Accesat pe 14.05.2023 la https://www.trendmicro.com/en_us/ciso/23/e/cyber-crime-group-types.html

46. TRENDMicro. 2019. “Cybecriminals”. Accesat pe 29.04.2023 la https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals.

47. Twitter – Dark Feed. 2023. “*Top active #ransomware groups june*” Accesat pe 10.07.2023 la https://twitter.com/ido_cohen2/status/1675905937524109325?S=20

48. Twitter - DarkFeed 2023. *„#Ransomware groups statistics March 2023*”. Accesat pe 10.07.2023 la https://twitter.com/ido_cohen2/status/1642218169765883907?s=20

49. Warminsky Joe. 2022. „*Notorious cybercrime gang Conti 'shuts down,' but its influence and talent are still out there*”. Therecord.media. Accesat la 05.05.2023 la https://therecord.media/conti-ransomware-gang-digital-infrastructure-shut-down

Aceasta este a doua ediție a volumului publicat de Academia Națională de Informații „Mihai Viteazul” (ANIMV), care cuprinde lucrările prezentate în cadrul Conferinței Științifice Intelligence și Cultura de Securitate 2023 (ICS2023). Inițiativa ICS2023 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 Informații și Securitate Națională 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