10.53477/2065-8281-22-84

MODUL ÎN CARE RĂZBOIUL DINTRE RUSIA ȘI UCRAINA POATE MODIFICA ECOSISTEMUL DE CRIMINALITATE CIBERNETICĂ

HOW THE RUSSIA-UKRAINE WAR MAY CHANGE THE CYBERCRIME ECOSYSTEM

Student doctorand Claudia–Alecsandra GABRIAN*

Potrivit statisticilor, în ultimii ani s-a înregistrat o creștere a atacurilor cibernetice și a impactului lor negativ asupra indivizilor, organizațiilor și guvernelor. Atacatorii cibernetici au dobândit resursele și expertiza necesară lansării de atacuri masive împotriva altor națiuni, cu scopul, în principal, de a câștiga avantaje strategice, țintind în special infrastructura critică și serviciile publice. Evenimentele geopolitice actuale, prin acțiunea lansată de Federația Rusă în Ucraina, demonstrează faptul că amenințările de securitate cibernetică sunt din ce în ce mai mari, iar răspunsurile statelor la aceste provocări trebuie să fie rapide și eficiente, adaptate acestui context. În ultimul an, grupările rusești de criminalitate cibernetică și-au consolidat poziția de amenințări la adresa ecosistemului digital global, demonstrând adaptabilitate, persistență și dorința de a exploata sistemele informatice. Lucrarea de față va analiza atât modalitățile în care grupurile de criminalitate cibernetică au fost mai prezente în spațiul internațional, ca urmare a acestui război, cât și importanța acordată acestora, din cauza tipurilor de atacuri lansate, precum și în ceea ce privește împărțirea lor în tabere de sprijin pentru beligeranți.

According to statistics, in recent years there has been an increase in cyber-attacks and their negative impact on individuals, organizations, and governments. Cyber attackers have acquired the resources and expertise to launch massive attacks against other nations to gain strategic advantages, mainly targeting critical infrastructure and public services. Current geopolitical events, through the action launched by the Russian Federation in Ukraine, demonstrate that cyber security threats are ever greater. States' responses to these challenges must be quick and effective, adapted to this context. Over the past year, Russian cybercrime groups have strengthened their position as threats to the global digital ecosystem, demonstrating adaptability, persistence, and a willingness to exploit computer systems. This paper will analyze how cybercrime groups have been more present in the international space due to this war, as well as the importance given to them due to the types of attacks launched and their division into belligerent support camps.

Cuvinte-cheie: atacuri cibernetice; grupuri de criminalitate cibernetică; ransomware; spațiu cibernetic; securitate cibernetică; reziliență.

Keywords: *Cyber Attacks; Cyber Crime Groups; Ransomware; Cyberspace; Cyber Security; Resilience.*

Spațiul cibernetic reprezintă un mediu de importanță strategică, ce este alcătuit nu doar din internet și din totalitatea tehnologiilor, respectiv a mijloacelor hardware și software, interconectate la nivel global, ci și din acțiunile derulate de utilizatorii acestora, care fac posibilă generarea, procesarea, stocarea sau transmiterea datelor în format electronic. Pentru a proteja astfel de sisteme, o mai bună înțelegere a criminalității cibernetice este o condiție necesară dezvoltării răspunsurilor adecvate prevenirii și combaterii acestor tipuri de amenințări. Acest fenomen al criminalității cibernetice are valențe la nivel global, depășește granițele geografice și poate fi realizat de oriunde, împotriva oricărei persoane și oricărei tehnologii. Nu există o definiție unică a termenului de criminalitate cibernetică, însă acesta descrie o varietate de infracțiuni ilegale sau ceea ce este considerat comportament ilicit de către indivizi/grupuri care lansează atacuri asupra dispozitivelor, rețelelor de tehnologie a informației, sistemelor și infrastructurii critice (Donalds și Osei-Bryson 2019).

Ca răspuns la aceste amenințări prezente și în continuă creștere, guvernele din întreaga lume au adoptat strategii și le-au aplicat prin

Universitatea Babeș-Bolyai
e-mail: *claudiaalecsandra@yahoo.com*

cadre legale în vederea stabilirii unei mai bune securități a computerelor, un exemplu concret fiind echipele de răspuns la incidente (CSIRT, denumite uzual CERT). Acestea investighează și previn astfel de tipuri de activități cibernetice ilicite, care implică utilizarea informațiilor și tehnologiile de comunicare (TIC). Potrivit lui Ngafeeson, clasificarea criminalității cibernetice este unul dintre cele mai importante trei elemente de combatere, iar Barn susține că o mai bună înțelegere a criminalității cibernetice este o condiție necesară dezvoltării unor răspunsuri adecvate și estimării corecte a costurilor economice, cu precădere (Donalds și Osei-Bryson 2019).

Sensul termenului „hacker” s-a modificat în timp, iar activitățile hackerilor sunt, de obicei, privite ca acțiuni ilegale care operează în medii ascunse, dar acest fapt este valabil atunci când provoacă daune intenționate sistemelor informaționale ale societății. Hackerii sunt principalii agenți ai criminalității cibernetice, iar subcultura lor este complexă și cuprinde multiple motivații, grade de idealism și seturi de abilități. Atacatorii sunt indivizi sau grupuri de persoane care încearcă să exploateze vulnerabilități, de cele mai multe ori pentru profit personal sau financiar, iar aceștia pot să lucreze pentru guverne, făcând spionaj pe noul câmp de luptă (Sabillon și alții 2016).

Hackingul devine ilegal odată ce trece peste pragul de obținere a accesului neautorizat la sistemele informatice. Hackerii sunt clasificați în mai multe categorii, cum ar fi: white hats, care lucrează în conformitate cu legile etice ale hackerilor sau ca experți în securitate; grey hats, care lucrează ca și consultanți de securitate; black hats, care sunt motivați de putere, furie sau ură, nu au nicio reținere în privința furtului sau distrugerii datelor din rețele. O altă categorie importantă sunt cyberteroriștii care fac parte din categoria celor care folosesc stenografia și criptologia pentru schimbul de informații și schimbul de date online, cu scopul de a fura informații cu valențe importante pentru societate, iar hackerii, ca agenți guvernamentali, sunt acele persoane sau grupuri care lucrează în scopuri guvernamentale specifice, care pot compromite securitatea cibernetică națională. Terorismul cibernetic este un alt element care face parte din construcția a ceea ce se numește criminalitate cibernetică și are în vedere acea clasă de teroriști cibernetici care exploatează vulnerabilitățile computerului. Atacatorii sunt motivați de ideologie politică, religie, tendințe hacktiviste sau cauze personale, iar furtul cibernetic îi are în vedere pe acei infractori cibernetici care caută profit financiar prin furtul și vânzarea informațiilor în toate modurile posibile (Sabillon și alții 2016).

Vulnerabilitățile cibernetice sunt exploatate prin atacuri cibernetice, iar faptul că tehnologia evoluează determină apariția de noi riscuri și amenințări care vor duce la mai multe tehnici, tactici și proceduri avansate (TTP) de hacking. În acest caz, sunt cunoscute amenințările persistente avansate (APT), care se referă la momentul în care un adversar posedă niveluri sofisticate de expertiză și resurse suficiente pentru a-și atinge obiectivele, folosind mai mulți vectori de atac prin selectarea țintei, cercetarea țintei, comandă și control, extragerea de date, informații diseminate și exploatarea informațiilor. Țintele infractorilor cibernetici sunt sectoarele infrastructurii critice, sistemul medical, sănătatea publică, sectorul tehnologiei informațiilor (IT), servicii financiare și energie (Sabillon și alții 2016).

Din categoria atacurilor cibernetice, menționăm: furtul de identitate, prin care atacatorul ia o falsă identitate pentru a obține beneficii financiare. Phishing este acea categorie de procese frauduloase care fură informații confidențiale de la utilizatorii care folosesc e-mailul spam. Distributed Denial-of-Service (DDoS) sunt acele atacuri care folosesc o rețea de mai multe sau chiar de mii de computere zombi care atacă o țintă specifică pentru a o suprasolicita în scopul nefuncționării. Atacurile malware sunt acele software-uri rău intenționate care sunt instalate prin intermediul diverșilor viruși, viermi, iar ransomware este o categorie a malware-ului care blochează datele utilizatorilor pentru a primi plata în vederea deblocării datelor (Sabillon și alții 2016).

Criminalitatea cibernetică este în continuă creștere, ca urmare a noilor tehnologii, cum ar fi inteligența artificială (AI). Din punctul de vedere al obținerii de profit financiar, formele de criminalitate cibernetică cele mai reprezentative sunt spionajul economic, furtul de proprietate intelectuală, crima financiară și ransomware. În ceea ce privește susținerea statelor cu privire la infractorii cibernetici, unele state sunt permisive și folosesc în scopuri interne informațiile obținute de aceștia,

spre exemplu Rusia, unde există o strânsă legătură între stat și crima organizată care îi protejează pe cei mai avansați criminali cibernetici. În Rusia sunt permise grupurilor de criminalitate cibernetică să-și urmărească scopurile financiare, le protejează de lege, însă în schimbul protecției, acestea trebuie să își folosească abilitățile pentru a susține interesele guvernului (Smith și Lostri 2022).

Grupările de criminalitate cibernetică

Spațiul cibernetic a devenit o zonă importantă de război, care are loc cu precădere pe internet, în care națiunile se pot lupta, fără să comaseze trupe și capabilități. Acest lucru permite țărilor cu o prezență militară redusă să fie la fel de puternice ca altele din spațiul cibernetic, prin penetrarea sistemelor informatice și a rețelelor altor națiuni. Acești atacatori au resursele și expertiza de a lansa atacuri masive pe internet împotriva altor națiuni, pentru a provoca daune sau pentru a întrerupe servicii, cum ar fi oprirea unei rețele energetice, dar și pentru a obține avantaje strategice. Prezența grupurilor de criminalitate cibernetică este mai pregnantă, acestea încercând să coopereze cu infractorii cibernetici (codificatori și hackeri) care au abilitățile esențiale pe care aceste grupuri le pot folosi sau de care au nevoie în anumite operațiuni.

Tehnologia informațiilor a transformat modul în care anumite grupuri sunt structurate și organizate, iar infractorii pot colabora la activitățile de hacking, folosind pseudonime, riscul dezvăluirii identității lor și a locațiilor către alți membri ai grupului fiind relativ scăzut. Una dintre principalele provocări este identificarea grupurilor de criminalitate cibernetică organizată, măsura în care aceste grupuri operează exclusiv, predominant și/sau parțial online (UNODC 2021). O națiune poate ataca infrastructura altei națiuni în mod constant, îi poate fura secretele militare și poate culege informații despre tehnologie, pentru a reduce decalajele industriale și militare, iar implicațiile dezvăluirii datelor cu caracter personal și accesul la date sensibile le oferă atacatorilor posibilitatea de a șantaja chiar personalul guvernamental (Neethu 2020).

Evenimentele geopolitice actuale, prin acțiunea lansată de Federația Rusă în Ucraina, au transformat lumea și oamenii au fost puși în fața unui război în Europa. Profitându-se de această oportunitate și urmărindu-se interese politice, economice și militare, amenințările de securitate cibernetică au devenit din ce în ce mai mari, iar provocările de securitate cibernetică sunt și vor fi în continuă evoluție. Securitatea persoanelor și a rețelelor cibernetice a căpătat o semnificație politică, în raport cu statul, cu societatea, cu națiunea și cu economia, iar vizarea în special a infrastructurilor critice se intersectează cu infrastructurile financiare, de transport, energetice și de securitate națională (Surdu 2018, 365-372).

Atacurile de ransomware și gruparea Conti

Figura 1 Modul de atac al ransomware (TrendMicro 2021)

În ultimul an, grupurile de criminalitate din Rusia și-au consolidat poziția de amenințări la adresa ecosistemului digital global, demonstrând adaptabilitate, persistență și dorința de a exploata sistemele informatice. Un atac de tip ransomware implică un software rău intenționat care implementează programe malware menite să cripteze și să exfiltreze date, păstrate în vederea unei răscumpărări, plata fiind adesea percepută în criptomonede. Mai mult decât atât, atacatorii exfiltrează date sensibile înainte de implementarea ransomware-ului pentru a împiedica victimele să se retragă de la negocieri. Potrivit statisticilor, actorii ransomware au trecut de la o abordare oportunistă cu volum mare la o metodologie mai selectivă în alegerea victimelor. Au crescut atacurile asupra sistemelor medicale, din cauza controalelor de securitate percepute ca fiind mai slabe și a tendinței

crescute a victimelor de a plăti răscumpărarea, din cauza criticității serviciilor lor. În plus, de la sfârșitul anului 2019, grupurile de ransomware au adoptat noi tactici de extorcare pentru a maximiza veniturile și au creat un stimulent suplimentar pentru ca victimele să plătească. Printr-o astfel de tactică, cunoscută sub numele de „extorcare dublă”, operatorii de ransomware exfiltrează cantități masive de date ale unei victime, criptându-le și apoi amenințând că le vor publica, dacă cererile de răscumpărare nu sunt îndeplinite (Financial Crimes Enforcement Network 2021).

A doua jumătate a anului 2021 a fost bogată în atacuri ransomware, acestea nu au fost doar foarte active, ci și foarte agresive. Dacă se are în vedere numărul de detectări per client activ pe țară, atunci obținem o distribuție ușor diferită. Tabelul următor arată procentul de clienți cu cel puțin o detectare de malware per țară în 2021, iar aici, se constată faptul că Republica Moldova a fost ținta atacurilor de malware încă din 2021. Acest lucru generează o serie de alte întrebări cu privire la faptul că Republica Moldova a fost vizată de mai multe atacuri cibernetice înainte ca războiul din Ucraina să înceapă, al căror răspuns conduce, de cele mai multe ori, atât la analiza evoluției atacurilor cibernetice, cât și a țintelor și schimbării acestora, determinând, cu precădere, o analiză amănunțită a scopului urmărit de aceste tipuri de atacuri, dar și a cauzelor pentru care Republica Moldova a reprezentat ținta unor astfel de atacuri.

Ransomware-ul este unul dintre cele mai profitabile atacuri cibernetice din acest moment, acesta se va extinde în continuare la macOS, Linux, precum și la noi medii, cum ar fi sistemele virtuale cloud și IoT, în ansamblu, orice lucru conectat la o rețea accesibilă fiind o țintă potențială (Acronis 2021). Majoritatea atacurilor de ransomware provin din Rusia sau de la aliații săi; majoritatea programelor ransomware vor încerca să vadă dacă rulează pe un computer o limbă comună vorbită în Rusia sau într-una dintre țările aliate ei, iar dacă răspunsul este favorabil, programul ransomware va renunța la atac. Unii atacatori recomandă activarea limbii ruse ca a doua limbă, dacă este posibil, pe computer, pentru a împiedica multe programe ransomware să se infiltreze. Rusia a devenit astfel o țară sigură din punct de vedere cibernetic, sau cum se mai numesc „paradisuri” pentru criminalii ransomware, iar astăzi, multe grupări de ransomware sunt situate în sau în jurul Rusiei (Grimes 2021). În perioada de raportare, frecvența și complexitatea atacurilor ransomware au crescut cu peste 150% și au devenit unele dintre cele mai mari amenințări cu care se confruntă organizațiile în prezent, indiferent de sectorul de care aparțin. Criptomoneda rămâne cea mai comună metodă de plată pentru acești actori, prin Monero, fiind metoda preferată, datorită anonimatului sporit și caracterului necunoscut al tranzacțiilor (ENISA 2021).

Rank	Country	Percentage of clients with malware detections in Q3 2021, normalized
1	Taiwan	63.6%
2	Singapore	57.4%
3	China	55.5%
4	Brazil	55.2%
5	Republic of Moldova	50.5%
6	Russia	49.5%
7	Greece	43.3%
8	Bulgaria	41.3%
9	South Korea	40.6%
10	Israel	39.7%
11	Turkey	39.4%

Figura 2 Detecții malware în țări (TrendMicro 2021)

Conti este un Ransomware-as-a-Service (RaaS) care a fost observat, pentru prima dată, în decembrie 2019, ca și în cazul altor familii de ransomware. Actorii care folosesc Conti fură fișiere și informații sensibile din rețele compromise și amenință să publice aceste date, dacă nu se plătește răscumpărarea (MITRE ATT&CK 2021). Agenția de Securitate Cibernetică și Securitate a Infrastructurii (CISA) și Biroul Federal de Investigații (FBI) au observat o utilizare crescută a ransomware-ului Conti în peste 400 de atacuri asupra SUA și organizațiilor internaționale. În atacurile tipice de tip ransomware Conti, actorii cibernetici rău intenționați fură fișiere, criptează servere și solicită răscumpărare. Pentru a securiza sistemele împotriva ransomware-ului Conti, CISA, FBI și Agenția Națională de Securitate (NSA) recomandă implementarea măsurilor de atenuare, care includ necesitatea de autentificare multifactor (MFA), implementarea segmentării rețelei și menținerea la zi a sistemelor de operare și a software-ului (CISA 2021).

Actorii Conti obțin adesea acces inițial la rețele prin campanii de spearphishing care utilizează e-mailuri personalizate care conțin atașamente rău intenționate sau linkuri rău intenționate. CISA și FBI au observat că gruparea Conti folosește Routerul Scan, un instrument de testare a pătrunderii, pentru a scana în mod rău intenționat routerele cu forță brută, camerele și dispozitivele de stocare atașate la rețea cu interfețe web. Actorii Conti sunt cunoscuți că exploatează software-ul legitim de monitorizare și management de la distanță și prin desktop. CISA și FBI au observat că actorii Conti folosesc diferite adrese IP ale serverului Cobalt Strike unice pentru victime diferite, iar după ce actorii fură și criptează datele sensibile ale victimei, folosesc o tehnică dublă extorcare prin care cer victimei să plătească o răscumpărare pentru eliberarea datelor criptate și amenință victima cu eliberarea publică a datelor, dacă răscumpărarea nu este plătită (CISA 2021).

Încă din 28 februarie 2022, actorii Conti au rămas activi și s-a raportat faptul că atacurile ransomware Conti împotriva organizațiilor americane și internaționale au crescut la peste 1.000, iar printre vectorii de atac notabili, se numără Cobalt Strike (CISA 2021). În luna mai, această grupare și-a închis platforma de operare și a avut loc o ierarhizare descentralizată, iar Departamentul SUA a oferit recompense de până la 10 milioane de dolari pentru orice informații care ar putea duce la identificarea unor persoane importante aparținând acestei grupări. După ce au atacat guvernul din Costa Rica și a fost instaurată alertă de securitate națională, această grupare a încetat voluntar la 19 mai 2022, în același timp având loc o reorganizare care avea să asigure o tranziție fără probleme a membrilor grupului de ransomware. Desființarea urmărea loialitatea publică a grupului față de Rusia în invazia Ucrainei, dând o lovitură uriașă operațiunilor sale din Ucraina și provocând scurgerea a mii de date private. Afilierea Conti la Rusia a avut și alte consecințe, principala consecință fiind incapacitatea sa de a extrage plăți de răscumpărare de la victime, din cauza sancțiunilor economice, impuse de Occident (The Hacker News 2022a).

După ce Conti a susținut public invazia Rusiei în Ucraina, un cercetător în domeniul securității cibernetice a identificat codul sursă al malware-ului și chaturile interne dintre afiliați și le-a făcut publice. Conti și Hive sunt, în prezent, poziționate ca doi dintre cei mai mari jucători de pe scena ransomware. Scurgerile Conti au vizat expunerea informațiilor interesante din interior între operatorii Conti, cum ar fi diverse locuri de muncă, rolurile în cadrul organizației și procesul de angajare a noilor afiliați. Pe baza jurnalelor de chat care au fost analizate între Conti și victime, sunt observate următoarele tehnici: stilul de comunicare al lui Conti este relativ profesional, marcat de introduceri, aparent scenarii, și de un ton lipsit de emoție. Actorii rămân pe mesaj, explicând victimei că sunt infectați, subliniind consecințele pe care le va suporta victima, dacă nu reușește să plătească răscumpărarea și încearcând să o convingă să plătească cât mai repede posibil (Mckay 2022).

Ultimele date cunoscute despre această grupare au în vedere faptul că foști membri ai grupului de criminalitate cibernetică Conti au fost implicați în cinci campanii diferite de atacuri care au vizat Ucraina, din aprilie până în august 2022. Potrivit Google Threat Analysis Group (TAG), sunt identificate acele activități cibernetice continue care vizează națiunea est-europeană, având ca și context războiul ruso-ucrainean. UAC-0098 este departe de a fi singurul grup de hacking afiliat Conti care a țintit Ucraina de la începutul războiului și care vizează organizații ucrainene și organizații

neguvernamentale (ONG) europene (The Hacker News 2022c). UAC-0098 este un broker de acces initial, cunoscut pentru utilizarea troianului bancar IcedID care oferă grupurilor de ransomware acces la sisteme compromise din rețelele întreprinderilor (Gatlan 2022). Un exemplu concret în acest sens este dat de echipa Ucrainei de Răspuns la Urgență Informatică, care a detectat un atac cibernetic asupra infrastructurii critice a Ucrainei, pe care l-a atribuit UAC-0098, însă acesta nu este singurul exemplu de atac cibernetic masiv care a fost orientat asupra Ucrainei și sistemelor de securitate ale țării (CyberSecurity Help 2022).

Modificarea ecosistemului de criminalitate cibernetică

Din cauza faptului că acest război este încă în desfășurare, impactul acestuia asupra spațiului cibernetic și asupra grupărilor de criminalitate cibernetică este unul considerabil prin prisma faptului că membrii grupărilor de criminalitate cibernetică își reorganizează strategiile de atac și operează mai mult în social media, pentru a atrage susținători. Apelul pe care aceștia îl fac este regăsit cu precădere la ambele tabere, iar Universitatea Australiană din Adelaide a descoperit milioane de tweeturi false de la o armată de boți proucraineni care răspândesc dezinformare și propagandă anti-rusă. Hashtagul #IStandWithUkraine a fost postat de boți cu o rată de 38.000 de tweeturi pe oră, iar după aceea numărul de tweeturi a crescut la 50.000 pe oră. Cercetătorii remarcă faptul că vârful de activitate al boților proucraineni a avut loc între orele 18:00 și 21:00, potrivit fusurilor orare din SUA (Gaskin 2022).

Hackerii fiind împărțiți în cele două tabere, proucrainieni și proruși, încearcă în mediul virtual să obțină sau să transmită cât mai multe informații care să influențeze într-un anumit mod cetățenii. O informație relevantă asupra acestui subiect are legătură, în principal, cu gruparea de hackeri Anonymous, care și-a declarat, încă de la începutul războiului, susținerea Ucrainei, iar astfel a atacat în masă sistemele de operare centrale ale diferitelor instituții și sisteme de stat ale Rusiei, un exemplu concret fiind Banca Centrală a Rusiei. În schimb, printre țintele hackerilor proruși, sunt și țări, pe lângă Ucraina, vizate, spre exemplu, Polonia, iar de cele mai multe ori, aceste tipuri de atacuri vizează industria transporturilor și infrastructura critică.

În ultimele luni, datorită eforturilor conexe ale instituțiilor de apărare și securitate din mai multe țări, a fost posibilă arestarea unor hackeri importanți din grupări precum LockBit și Killnet, care erau urmăriți penal pentru atacuri împotriva mai multor instituții și organizații. Atacurile cibernetice majore au vizat și serviciile de informații ale unor țări, cum ar fi: Estonia, Polonia, România, Bulgaria și Moldova. Spre exemplu, grupul prorus Killnet și-a asumat responsabilitatea pentru mai multe atacuri cibernetice, dintre care un atac asupra site-ului web și asupra serviciilor sistemului electronic federal de plăți fiscale din SUA. De asemenea, gruparea Hive a atacat peste 1.300 de companii din întreaga lume și a vizat o gamă largă de întreprinderi și sectoare critice de infrastructură, inclusiv facilități guvernamentale, comunicații, producție critică, tehnologia informației, sănătate și sănătate publică (The Hacker News 2022b).

Odată cu începerea războiului, ecosistemul de criminalitate cibernetică s-a orientat spre atacarea Ucrainei, cu precădere, iar astfel, s-a creat o armată IT a Ucrainei, care este estimată la aproximativ 215.000 de afiliați, formată din voluntari, care vizează instituțiile media rusești, sponsorizate de stat. Armata a executat atacuri cibernetice asupra a aproximativ 8.000 de resurse rusești, vizând cu succes industria de apărare și contracarând campaniile de dezinformare ale instituțiilor sponsorizate de stat. Președintele ucrainean, Volodimir Zelenski, a menționat că armata IT a Ucrainei a prevenit cu succes peste 1.300 de atacuri cibernetice rusești în ultimele opt luni ale invaziei ruse. De exemplu, după ce Rusia a distrus un important centru de date din țară, Ucraina a trecut la sistemul cloud, permițându-i să construiască registre publice și să facă plăți către cetățenii afectați de război (Dark Reading 2022).

Până acum, grupările de criminalitate cibernetică modifică acest ecosistem prin orientarea atacurilor asupra Ucrainei și țărilor care o susțin, prin schimbarea manierei de atac a potențialelor ținte. Faptul că se apelează la mobilizarea populației în social media pentru a atrage sute de mii de oameni înspre hacktivism nu face altceva decât să demonstreze că războiul se regăsește și în spațiul cibernetic, trece de granițele normale ale unui teritoriu și are valențe globale. Prognozele cu privire la aceste tipuri de atacuri cibernetice au în vedere amploarea lor și

modalitatea în care aceste grupări vor acționa, dar și modul în care țările potențial vizate de acestea vor implementa strategii care să prevină atacuri cibernetice majore, cu precădere asupra infrastructurilor critice.

Concluzii

În concluziile articolului, se pot menționa următoarele aspecte care să justifice subiectul cercetat; astfel, se constată că atacurile cibernetice sunt din ce în ce mai complexe, iar războiul din Ucraina reprezintă o sursă de motivație pentru a susține sau nu beligeranții de către grupările de criminalitate cibernetică, de unde și împărțirea acestor grupări în tabere. Grupurile ransomware au avut activitate încă din 2020, iar în Federația Rusă este recunoscut faptul că grupările de criminalitate cibernetică primesc susținere, pentru ca, ulterior, acestea să acționeze în interesul statului. Gruparea Conti este relevantă pentru a analiza modalitarea în care războiul actual poate modifica ecosistemul de criminalitate cibernetică, deoarece această grupare, relativ nouă, care a susținut și a acționat împotriva statelor care nu susțin acțiunea Rusiei a fost divizată doar în urma mai multor atacuri cibernetice lansate, pentru ca, ulterior, acestea să fie reluate sub o altă identitate, dar, în esență, urmărind același scop. În Rusia, operațiunile ofensive sunt ajutate de tehnologia avansată, cum ar fi inteligența artificială (AI) și automatizarea, pentru a oferi comandă și control, iar astfel, spațiul cibernetic poate fi privit drept un teren mult mai avantajos în războiul hibrid, pe care aceste grupări să îl exploateze. Faptul că Rusia încearcă să izoleze internetul rusesc de cel global este un exemplu pentru a justifica înarmarea Rusiei din interior, pentru a-și practica activitățile cibernetice care să vizeze țările adversare. Acest lucru i-a sporit influența geopolitică și a contribuit la amplificarea puterii sale de jucător pe scena internațională. Geopolitica este un instrument esențial și indispensabil pentru înțelegerea și analizarea noilor provocări cibernetice, iar principalul factor în această dinamică este politica, geopolitica fiind cea care interacționează și determină scopul atacului cibernetic. Sistemul internațional poate să rămână unul în care deziderateleț țărilor membre să fie în concordanță cu apărarea și integritatea spațiului cibernetic și cu siguranța sistemelor informatice și a infrastructurii critice, însă zona de amenințări hibride va fi una mai exploatată și mai potențială pentru actorii statali sau nonstatali, care, probabil, vor face presiuni asupra economiei, politicii, infrastructurilor critice, cetățenilor etc.

BIBLIOGRAFIE

Acronis. 2021. ”Acronis Cyberthreats Report 2022 unveils cyberthreat predictions.” https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-2022-unveils-cyberthreat-predictions/.

CISA. 2021. ”AA21-265A-Conti Ransomware TLP White.” https://www.scribd.com/document/529330620/AA21-265A-Conti-Ransomware-TLP-WHITE.

CyberSecurity Help . 2022. ”Former Conti Hackers Adapt Their Techniques to Use against Ukraine.” https://www.cybersecurity-help.cz/blog/2878.html.

Dark Reading. 2022. ”Ukraine’s ‘IT Army’ Stops 1,300 Cyberattacks in 8 Months of War.” https://www.darkreading.com/endpoint/ukraine-it-army-stops-1300-cyberattacks-war.

Donalds, Charlette și Kweku-Muata Osei-Bryson. 2019. ”Toward a Cybercrime Classification Ontology: A Knowledge-Based Approach.” *Computers in Human Behavior* 92: 403-418. doi:https://doi.org/10.1016/j.chb.2018.11.039.

ENISA. 2021. ”Enisa Threat Landscape 2021.” https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

Financial Crimes Enforcement Network. 2021. ”Financial Trend Analysis.” https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomeware%20508%20FINAL.pdf.

Gaskin, Lee. 2022. ”Bots Manipulate Public Opinion in Russia-Ukraine Conflict.” *The University of Adelaide.* https://www.adelaide.edu.au/newsroom/news/list/2022/09/08/bots-manipulate-public-opinion-in-russia-ukraine-conflict.

Gatlan, Sergiu. 2022. ”Google Says Former Conti Ransomware Members Now Attack Ukraine.” *BleepingComputer.* https://www.bleepingcomputer.com/news/security/google-says-former-conti-ransomware-members-now-attack-ukraine/.

Grimes, Roger A. 2021. *Ransomware Protection Playbook.* John Wiley & Sons Inc.

Mckay, Kendall. 2022. ”Conti and Hive ransomware operations: Leveraging victim chats for insights.” https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf?1651576098.

MITRE ATT&CK. 2021. ”Conti.” https://attack.mitre.org/software/S0575/.

Neethu, N. 2020. ”Role of International Organizations in Prevention of Cyber-Crimes: An Analysis.” Nalsar University of Law, Hyderabad, 5-17. https://www.researchgate.net/profile/Neethu-N-2/publication/350525198_Role_of_International_Organisations_in_Prevention_of_Cyber-Cri.

Sabillon, Regner, Victor Cavaller, Jeimy Cano și Jordi Serra-Ruiz. 2016. ”Cybercriminals, Cyberattacks and Cybercrime.” *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF).* 1-9. doi: https://doi.org/10.1109/icccf.2016.7740434.

Smith, Zhanna Malekos și Eugenia Lostri. 2022. ”The Hidden Costs of Cybercrime.” https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

Surdu, Ileana-Cinziana. 2018. ”Cybersecurity. Risks, Threats, and Trends of Manifestation in Romania.” *International Conference RCIC’18.* 365-372. https://www.afahc.ro/ro/rcic/2018/rcic’18/volum_2018/365-372%20Surdu.pdf.

The Hacker News. 2022a. ”Conti Ransomware Operation Shut down after Splitting into Smaller Groups.” https://thehackernews.com/2022/05/conti-ransomware-gang-shut-down-after.html.

—. 2022b. ”Hive Ransomware Attackers Extorted $100 Million from over 1,300 Companies Worldwide.” https://thehackernews.com/2022/11/hive-ransomware-attackers-extorted-100.html.

—. 2022c. ”Some Members of Conti Group Targeting Ukraine in Financially Motivated Attacks.” https://thehackernews.com/2022/09/some-members-of-conti-group-targeting.html.

TrendMicro. 2021. ”Toward a New Momentum: Trend Micro Security Predictions for 2022.” https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2022.

UNODC. 2021. ”Digest of Cyber Organized Crime.” https://www.unodc.org/documents/organized-crime/tools_and_publications/21-05344_eBook.pdf.