INTELLIGENCE ȘI CULTURA DE SECURITATE

CONFERINȚA ȘTIINȚIFICĂ STUDENȚEASCĂ

PROCEEDINGS

VOLUMUL 3
2024

Editura Academiei Naționale de Informații
„Mihai Viteazul”

NOILE PROVOCĂRI ÎN ECOSISTEMUL DE CRIMINALITATE CIBERNETICĂ

Claudia-Alecsandra GABRIAN[*]

Abstract:

The current cyber threat landscape can be influenced by geopolitical dynamics that can lead to substantial challenges. Many organized cyber criminals continue to develop their threat operations to execute high-impact attacks by extorting ransoms, disrupting governments, critical services, and exposing sensitive data. This article aims to identify in which manner the ransomware groups are expected to explore new skills and how they can integrate Artificial Intelligence (AI) in their attacks. Another purpose is to identify how they can exploit global events and how the attacks in 2023 can be connected in 2024. The cybercriminal group that was chosen for this research is LockBit ransomware because according to the statistics from 2023, it is the most prolific cybercriminal ransomware group. Even though the main focus of this article is LockBit, there is one exception, because LockBit was disrupted by the FBI in February 2024 and another purpose is to identify how they can continue their attacks after the disruption. The main results are that cybercriminals use AI malware to execute more highly developed cyberattacks shortly and 2024 can be a year where ransomware attacks can predominate through new LLM models. This paper's main conclusions are that cybercriminals continue to launch sophisticated ransomware attacks, and they can target global events, for example: elections in the US, European Union, Olympic games, and the current military conflicts can represent significant opportunities for cyber actors.

Keywords: *ransomware, artificial intelligence, cyberattacks, LockBit, geopolitical landscape.*

Introducere

Interconectivitatea devine un avantaj pentru grupările de criminalitate cibernetică, deoarece acestea utilizează toate instrumentele de care dispun pentru a maximiza efectul atacurilor pe care le lansează, ajungând de la un singur calculator compromis, să transfere atacul pe toate sistemele asoaciate. Acest aspect poate fi considerat o provocare pentru societate şi pentru cetăţeni, companii, guverne, instituţii de

[*] Universitatea Babeş-Bolyai, Facultatea de Istorie şi Filosofie, specializarea RISE, Cluj-Napoca, claudiaalecsandra@yahoo.com

securitate națională și cibernetică etc., deoarece având o gamă extinsă de aplicații augumentate, aceștia pot să devină mai specializați, iar vectorii de atac să fie mai greu de identificat. Atacurile de tip ransomware sunt printre cele mai preferate de către grupările de criminalitate cibernetică, deoarece prin cererea unei răscumpărari, aceștia pot să își sponsorizeze mai departe atacurile și să împartă cu afiliații sumele obținute. Noutatea apare atunci când sunt identificate din ce în ce mai multe atacuri cibernetice care utilizează instrumentele inteligenței artificiale pentru a fi mai inovativi și pentru a lansa atacuri mai avansate.

Stadiul actual al cercetării este unul avansat și relevant pentru domeniul studiat, deoarece oferă o contextualizare a amenințărilor persistente, regăsindu-se perpective esențiale pentru identificarea modului în care inteligența artificială poate să fie utilizată de către criminalii cibernetici. De asemenea, evidențierea modului în care grupările de criminalitate cibernetică pot să se implice în procese electorale și să influențeze alegătorii, urmărind interese geopolitice. Un alt exemplu este gruparea LockBit care a atras atenția la începutul acestui an cu privire la sistarea site-ului acesteia, iar faptul că încă este activă și va lansa în curând o nouă versiune de operare, reprezintă un exemplu relevant în analizarea ecosistemului de criminalitate cibernetică și a modului în care gruparea care a ocupat locul 1 în statistica din anul 2023 poate să operaționalizeze în continuare.

Scopul acestui articol este de a evidenția care ar putea fi cele mai recente sau viitoare amenințări cibernetice, cu precădere cele care sunt dezvoltate cu ajutorul inteligenței artifciale, cât și evenimente de importanță majoră, evaluând totodată impactul pe care ar putea să îl aibă acestea în ecosistemul cibernetic. Securitatea globală se confruntă cu provocări mai persistente, unde infractorii cibernetici reușesc să își continue activitatea, chiar dacă sunt vizați de către agențiile de securitate globale, cum este și cazul LockBit. Această grupare va reprezenta unul dintre subiectele centrale ale lucrării, deoarece analizând-o încă din anul 2019, au durat aproximativ 5 ani până când a fost identificată o vulnerabilitate sistemică (PHP) și au putut fi vizați prin operațiunea Cronos în 2024.

Obiectivul principal al acestui articol are în vedere enunțarea clară și concisă a sistemului ransomware prin gruparea LockBit, cât și impactul pe care atacurile cibernetice ar putea să le aibă la evenimentele importante din acest an, cum ar fi alegerile care vor fi organizate global și evenimentul cel mai așteptat, adică Jocurile Olimpice de la Paris. Analizând aceste evenimente se pot stabili anumite puncte comune care

au fost identificate în trecut, cât şi care va fi evoluţia lor în timp, având în vedere faptul că tensiunile geopolitice sunt prezente, iar aceste evenimente sunt preferate de către grupările de criminalitate cibernetică pentru a exploata şi identifica date sensibile pe care mai târziu să le monetizeze. De asemenea, spionajul cibernetic realizat de către grupări asociate cu servicii de securitate ruse reprezintă o ameninţare persistentă, care trebuie să fie identificată din timp şi prevenită.

În cadrul metodologiei utilizate în acest articol, se vor regăsi două metode de cercetare specifice, prima este netnografia, iar a doua este analizarea documentelor oficiale asociate cu domeniul criminalităţii cibernetice şi publicate de către instituţiile abilitate în acest domeniu. Utilizarea acestor două metodologii complementare ajută la obţinerea unei înţelegeri aprofundate a ecosistemului de criminalitate cibernetică, cât şi a fenomenelor care sunt în continuă evoluţie. Prima metodă de cercetare, netnografia, este utilizată pentru a realiza o analiză bazată pe observaţia participativă în cadrul canalelor de comunicare ransomware, pentru o mai bună înţelegere a dinamicii din cadrul grupărilor şi a afiliaţilor. A doua metodă de cercetare, analiza documentelor, este utilizată pentru a examina şi interpreta tipuri de documente, cum ar fi cele oficiale, articole şi mesaje postate chiar de către membrii grupărilor de criminalitate cibernetică, aşa cum este şi mesajul postat în limba rusă de către liderul LockBit după ce le-a fost sistată activitatea în februarie 2024.

În cadrul acestui articol, întrebarea de cercetare defineşte scopul şi direcţia cercetării, iar informaţiile regăsite vor fi orientate înspre identificarea evenimentelor care să răspundă întrebării de cercetare propuse: "Care sunt evenimentele-cheie din anul 2024 care pot să influenţeze ecosistemul de criminalitate cibernetică în 2024?". Această întrebare având rolul de a evidenţia importanţa evenimentelor din anul 2024, impactul pe care aceste evenimente îl vor avea asupra tuturor părţilor implicate şi enunţarea tuturor factorilor globali şi a acelor tendinţe care ar putea să influenţeze ecosistemul de criminalitate cibernetică.

Contribuţiile proprii se evidenţiază prin obţinerea de perspective noi cu privire la ecosistemul de criminalitate cibernetică prin analizarea grupărilor de ransomware, un avantaj însemnând înţelegerea limbii ruse pentru analizarea textului propriu-zis. De asemenea, subiectul cercetat este unul care în vedere aspecte relevante regăsite în ecosistemul de criminalitate cibernetică şi care pot să influenţeze viitoarele evenimente pentru anul 2024, deoarece sunt evenimente cu un impact geopolitic semnificativ, cât şi de interes la nivel global.

În anul 2023 atacurile cibernetice, cât şi nivelul de avansare al acestora a fost într-o linie ascendentă, iar acţiunile geopolitice au în continuare un impact major asupra acestora. Ameninţările ransomware au fost identificate în cadrul mai multor sectoare, iar peisajul cibernetic a devenit mai diversificat, în compaţie cu anul 2022. Atacatorii cibernetici continuă să îşi dezvolte operaţiunile pentru a executa atacuri cu un impact major pentru a afecta guverne, servicii critice şi pentru a expune date sensibile, în scopul de a obţine câştiguri financiare prin răscumpărarea pe care o solicită pentru aceste date (SentinelOne,2023). În prezent aceştia realizează activitităţi rău intenţionate, au obiective strategice şi sunt orientaţi înspre profit, astfel devin entităţi rationale care caută vulnerabilităţi în sistemele informatice care să le ofere un venit constant. Pentru anul 2024, evoluţia ameninţării ransomware poate fi privită din perspectiva utilizării inteligenţei artificiale şi mai multe exploatării de tip zero-day (Bitdefender,2024).

Grupările de criminalitate cibernetică lansează atacuri multi-motivaţionale, urmărind beneficii politice sau financiare prin vizarea alegerilor electorale şi evenimentelor de amploare globală, cum ar fi Jocurile Olimpice. Manipularea alegerilor se poate realiza prin mai multe tehnici, prima etapă o reprezintă campaniile de dezinformare care ulterior se transformă în interferenţe directe asupra sistemelor de vot pentru a influenţa opinia alegătorilor, în timp ce altele afectează voturile în sine. Motivele de cele mai multe ori sunt asemănătoare în ambele cazuri, însă în cazul Jocurilor Olimpice, există şi altele care au în vedere atragerea atenţiei globale prin atacuri asupra sistemelor de bilete, transmisiilor de evenimente sau furtul de date cu caracter personal ale sportivilor şi participanţilor.

1. Ecosistemul ransomware

Ameninţările ransomware vor fi mult mai sofisticate şi vor evolua în 2024. Grupările de ransomware vor implementa vulnerabilităţi zero-day; prin urmare, sistemul care este neactualizat sau nu are o protecţie suficientă va fi uşor de compromis. Un alt aspect este eficienţa procesului de identificare şi de triaj a victimelor. Grupările de ransomware vor aloca mai multă atenţie pentru a verifica potenţialele ţinte în scopul maximizării profitului, în special vizând companiile mari din sectorul de producţie sau de asistenţă medicală esenţială. Aceste grupări vor continua să folosească forme avansate de tehnici de criptare; în ultimul an criptarea post-cuantică a fost adoptată pentru a face atacurile şi mai greu de contracarat (Bitdefender, 2024).

Modernizarea codului ransomware este o nouă provocare în peisajul ameninţărilor, deoarece atacatorii adoptă un limbaj de programare Rust, dar şi Go şi Swift. Programul Rust le permite să scrie un cod mai sigur care poate fi compilat în diferite sisteme de operare. Acesta nu criptează complet fişierele, favorizează criptarea intermitentă şi poate să folosească criptarea cuantică. Două avantaje importante constau în primul rând în faptul că devine mai dificil pentru instrumentele de securitate să detecteze atacul datorită similitudinii statistice dintre fişierul criptat parţial şi cel original; iar în al doilea rând, procesul de criptare este mai rapid, permiţând ransomware-ului să cripteze mai multe fişiere într-un anumit interval de timp (Bitdefender,2024).

O altă provocare constă în faptul că pentru modelul de afaceri ransomware-as-a-Service (Raas), grupările recrutează activ membrii cu abilităţi avansate şi studii superioare pentru a avea specilişti în domeniu care să execute atacuri din ce în ce mai sofisticate, iar pe urmă profitul să se impărtă în funcţie de aportul fiecăruia în procese. De asemenea, peisajul competitiv dintre aceştia se va intensifica, deoarece între aceste grupări vor apărea discuţii cu privire la menţinerea reputaţiei, devenind astfel o vulnerabilitate pentru operaţiunile lor şi în cadrul grupărilor (Bitdefender,2024).

Dark web este un habitat pentru criminalitatea cibernetică, iar dintre toate reţelele sale anumite platforme se remarcă prin influenţă şi anonimatul pe care îl oferă. O atenţie deosebită este acordată forumurilor dark web care operează în limba rusă, deoarece deţin o poziţie unică datorită bazei lor extinse de utilizatori şi a complexităţii operaţiunilor lor. Aceste forumuri nu sunt doar platforme pentru activităţi ilegale; ele oferă surse critice de informaţii pentru instituţiile de aplicare a legii şi pentru cercetări. Prin monitorizarea acestor platforme, se pot obţine cu uşurinţă informaţii despre ameninţări, despre membrii platformei şi despre planurile şi discuţiile pe care le au (SOCRadar, 2024).

Un exemplu de platformă care este una dintre cele mai recunoscute şi profesioniste platforme în ecosistemul de criminalitate cibernetică, este XSS.is care începând cu 2013 până în prezent a devenit un pion important în acest peisaj. Acest forum privat, unde se vorbeşte limba rusă, operează atât la suprafaţă, cât şi pe dark web şi oferă un mediu anonim şi sigur pentru cei care vor să se înscrie. Această platformă a devenit în timp un spaţiu de încredere pentru activităţile infracţionale cibernetice. XSS.is dezactivează jurnalele adreselor IP şi criptează mesajele private, pentru a oferi anonimat utilizatorilor. Chiar dacă în 2021 au fost interzise discuţiile despre ransomware, platforma şi-a dezvoltat o reputaţie

în jurul punctelor de recrutrare și de întâlnire dintre cele mai cunoscute grupări de ransomware, chiar și LockBit (SOCRadar, 2024).

2. Gruparea ransomware LockBit

Din anul 2019, gruparea ransomware LockBit rulează drept ransomware-as-a-service (RaaS), unde criptatorii sunt recunoscuți drept afiliați care efectuează atacurile în schimbul unei reduceri din veniturile răscumpărării. Atacurile urmează o tactică numită extorcare triplă pentru a fura date sensibile înainte de a le cripta, iar aceștia exercită presiuni asupra victimelor pentru a efectua o plată pentru a-și decripta fișierele și pentru a preveni publicarea datelor lor. LockBit este una dintre grupările de ransomware care acceptă criptarea de la distanță, un avantaj semnificativ peste aceștia este faptul că nu se poate detecta activitatea rău intenționată, deoarece este prezentă doar într-un dispozitiv negestionat. Această dezvoltare a criptării de la distanță vine pe fondul unor schimbări în peisajul ransomware-ului, deoarece sunt utilizate noi limbaje de programare, iar lansarea atacurilor cibernetice sunt programate după orele de muncă sau la sfârșit de săptămână pentru a nu fi detectate (The Hacker News,2024).

LockBit 3.0 sau LockBit Black este ultima variantă de operare care folosește modelul Ransomware-as-a-Service (RaaS), iar potrivit ultimului raport ENISA care are în vedere perioada iulie 2022-iunie 2023, gruparea LockBit a ocupat primul loc în rândul atacurilor cibernetice, având o rată de peste 1000 de atacuri cibernetice, iar din 2019 până în februarie 2024 nu a fost sesizată de către forțele de ordine (ENISA,2023). În comparație cu gruparea CL0P, aceasta a compromis peste 3.000 de organizații din SUA și 8.000 de organizații globale, doar în anul 2023, ceea ce a dus la detronarea grupării LockBit de pe prima poziție pentru câteva luni. Prin cele două vulnerabilități zero-day MOVEit și GoAnymwhere, gruparea a avut una dintre cele mai mari campanii de amenințare din 2023, ceea ce a dus la alertarea instituțiilor competente pentru a oferi recompense oricărei persoane care poate să ofere informații veridice despre ei, care ulterior să conducă la arestarea membrilor grupării.(SentinelOne, 2023) După atacurile zero-day, gruparea CL0P a adoptat o altă tactică față de cea obișnuită, după reușita multitudinii de atacuri, s-a retras de pe scena amenințărilor cibernetice, iar până în prezent nicio altă gruparea de ransomware nu a reușit să detroneze LockBit, până la CL0P (SOCRadar,2024).

LockBit a fost implicată în numeroase incidente de securitate asupra organizațiilor la nivel global de-a lungul anilor. Într-o configurație

tipică RaaS, câştigurile sunt împărţite atât între dezvoltatori, cât şi afiliaţi, după ce răscumpărarea a fost negociată şi plătită. LockBit percepe în mod normal o cotă de 20% din răscumpărare per victimă plătitoare, restul de 80% fiind acordat afiliatului. Cu toate acestea, dacă LockBit însuşi este cel care conduce negocierile, această taxă creşte de la 30 până la 50%. În noiembrie 2023, gruparea a introdus noi recomandări pentru răscumpărare bazate pe veniturile victimei, interzicând reduceri de peste 50%. Din punct de vedere pur tehnic, LockBit a abordat o altă tactică, are o capacitate de auto-răspândire. Odată ce o gazdă din reţea este infectată, LockBit este capabil să caute alte ţinte din apropiere şi să încerce să le infecteze. Gruparea s-a evidenţiat prin fenomene atipice, cum ar fi plătirea oamenilor pentru a-şi face tatuajele LockBit şi chiar oferirea unei recompense de 1 milion de dolari pentru oricine ar putea afla identitatea în lumea reală a liderului LockBit (SOCRadar,2024). În special, LockBit a publicat pe forumul XSS recompensele pentru tatuajele LockBit.

O operaţiune internaţională care include Europol şi 11 ţări, a confiscat cu succes domeniile darknet ale grupării LockBit. Primul anunţ al vizării a fost făcut de Agenţia Naţională a Criminalităţii din Marea Britanie (NCA) care a confirmat că a obţinut codul sursă LockBit, precum şi o mulţime de informaţii referitoare la activităţile sale şi afiliaţii acestora, ca parte a unui grup operativ dedicat, numit Operaţiunea Cronos. În sistemele regăsite s-a identificat faptul că unele date aparţineau victimelor care au plătit răscumpărarea, ceea ce înseamnă că datele sunt stocate chiar dacă este plătită răscumpărarea, ceea ce nu respectă garanţia ştergerii datelor propusă de atacatori. De asemenea, au fost arestaţi doi membri LockBit în Polonia şi Ucraina. Sancţiuni au fost stabilite în SUA împotriva altor doi cetăţeni ruşi despre care se presupune că ar fi comis atacuri LockBit, pe nume Artur Sungatov şi Ivan Gennadievich Kondratiev (alias Bassterlord). Agenţia a reuşit să preia controlul asupra serviciilor LockBit şi s-a infiltrat în întregul său sistem datorită unei vulnerabilităţi identificate PHP. 34 de servere aparţinând afiliaţilor LockBit au fost şi ele sesizate şi peste 1.000 de chei de decriptare au fost recuperate de pe serverele LockBit confiscate (SOCRadar,2024).

Cu toate acestea, LockBit a reapărut pe dark web cu o nouă infrastructură la scurt timp după ce le-au fost confiscate serverele. Aceştia şi-au mutat serverele Tor la o nouă adresă .onion şi a postat 12 noi victime pe portalul său de scurgeri de date şi a discutat despre exploatarea unei vulnerabilităţi PHP care a dus la sesizarea serverului intern (The Hacker News, 2024). După atac, personalul administrativ al grupării de ransomware

Lockbit a informat că lucrează activ la mai multe proiecte noi și au dezvoltat o nouă sarcină de ransomware care vizează platforma cloud Nutanix. În urma evenimentului, LockbitSupp a înaintat o scrisoare către FBI și a amenințat că va publica date care au fost obținute în urma atacului asupra Comitatului Fulton din Georgia, atac care a fost realizat de către unul dintre afiliații lor. Aceste date sunt sensibile din cauza faptului că l-ar inculpa pe Donald Trump, iar astfel LockbitSupp susține că „Operațiunea Kronos" a fost efectuată pentru a preveni publicarea datelor care ar putea afecta alegerile viitoare. LockBit a postat un articol pe noul server, care a fost scris de către liderul său, acesta a promis să nu se retragă din lumea criminalității subterane, iar acesta a recunoscut motivul pentru care au fost vizați, acela că în ultimii 5 ani fiind obișnuiți cu recompense din ce în ce în mai mari, "au devenit leneși" (BankInfoSecurity,2024).

În prezent există o versiune în curs de dezvoltare a ransomware-ului numit LockBit-NG-Dev, care ar putea fi o versiune viitoare pe care gruparea ar putea să o considere versiunea 4.0 după ce este finalizată. Aceasta este o versiune în dezvoltare a unui malware în testare independent de platformă, care este diferită de versiunile anterioare. Eșantionul adaugă un sufix „locked_for_LockBit" la fișierele criptate care, fiind parte a configurației și, prin urmare, aceasta ar putea să fie o versiune viitoare neimplementată de grupare. Pe baza stării sale actuale de dezvoltare, se urmăresște activ variantă LockBit-NG-Dev (TrendMicro, 2024).

Interesant este faptul că o grupare de ransomware nou descoperită numită Red CryptoApp și-a început operațiunile între februarie și martie anul acesta, ceea ce coincide cu operațiunile de sesizare asupra Lockbit. Raportul de victimologie pentru Red Ransomware dezvăluie o gamă restrânsă de victime în câteva sectoare și țări, publicându-le pe site-ul său Data Leaks (DLS). Odată ce un sistem este compromis, toate fișierele sunt modificate cu extensia .REDCryptoApp, făcându-le inaccesibile. Aceștia utilizează text generat de AI în comunicarea cu victimele, ceea ce înseamnă o evoluție a operațiunilor ransomware (SOCRadar,2024).

3. Inteligența artificială și atacurile cibernetice

Principiul inteligenței artificiale asociat cu criminalitatea cibernetică poate fi identificat în momentul în care atacatorii cibernetici își ajustează instrumentele de hacking pentru a penetra sisteme și pentru a trece neobservați. AI le poate ușura munca acestora și de asemenea poate fi considerată un nou risc pentru sistemele informatice. Predicțiile despre integrarea AI în atacurile de timp ransomware poate să fie imprevizibilă

deoarece poate fi folosit atât ca un instrument care să imbunătăţească abilitiţările existente ale atacatorilor, cât şi să fie programat pentru a realiza atacuri de unul singur ceea ce va duce la o identificare mai dificilă dacă un atac este executat de un actor sau este oferită asistenţă AI. Până în prezent, satisfacţia hackerilor cu privire la dezvoltarea de către AI a codului malware este una nemulţumitoare. Calitatea codului de malware tinde să fie scăzută, deci chiar dacă acest cod poate să fie scris de AI, ajunge să fie o opţiune mai puţin selectată de către hackerii cu experienţă (Bitdefender,2024).

Implicarea LLM-urilor va reprezenta un prim pas înspre următoarea etapă a utilizării instrumentelor AI care vor deveni din ce în ce mai frecvente. Aceste LLM-uri sunt modele de limbaj, fiind programe de inteligenţă artificială (AI) care pot să recunoască şi pot genera text, printre alte sarcini, cum este de exemplu ChatGPT (Cloudflare,n.d.). Aceste mesaje pot să devină mai persuasive şi mai realiste, ceea ce reiese faptul că nu se mai poate face diferenţa între mesajele autentice şi cele generate. Eliminarea barierelor lingvistice poate duce la extinderea activităţilor acestora către un public mai larg, cât şi să permită actorilor care au deja competenţe să execute atacuri mai sofisticate. Aceşti infractori cibernetici pot să creeze LLM-uri personalizate care să reprezinte o ameninţare pentru cetăţeni, de asemenea pot să folosească versiuni personalizate ale GPT Builder oferit de OpenAI pentru a-i asista pe aceştia în atacurile pe care le realizează (Bitdefender,2024).

O altă provocare adusă de utilizarea AI sunt deepfake-urile, care devin din ce în ce mai convingătoare, utilizând imagini audio şi video în care sunt prezente personalităţi cunoscute, politicieni, fondatori de opinie etc. Aceste deepfake-uri alimentează campaniile de dezinformare, ceea ce necesită de asemenea o atenţie sporită a instituţiilor care se asigură de protejarea spaţiului cibernetic (Bitdefender,2024).

O provocare o reprezintă utilizarea open source intelligence (OSINT) cum ar fi Havok şi Sliver, prin care se pot obţine mai multe informaţii cu privire la un anumit subiect. Infractorii cibernetici folosesc acest tip de căutare, deoarece pot să primească răspunsuri la multe întrebări pe care le au. În ceea ce priveşte cazul ransomware, aceste grupări includ OSINT pentru a evalua şi a determina care sunt cele mai adecvate cereri de răscumpărare. Prin utilizarea LLM-urilor se pot colecta informaţii despre companii, instituţii, întreprinderi etc. Una dintre cele mai practice şi mai uşor de monetizat utilizări ale AI este dezvoltarea unui instrument de recunoaştere bazat pe inteligenţă artificială pentru a analiza cantităţi mari de date şi a identifica ţinte valoroase cu capacităţi

financiare semnificative. Prin selectarea și țintirea organizațiilor cu cel mai mare potențial de a plăti răscumpărări substanțiale, grupările de ransomware și-ar putea crește cererile maxime de răscumpărare, ceea ce duce la venituri potențial mai mari ale acestora (Bitdefender,2024).

4. Influența pe care o au grupările de cybercrime în evenimente globale

Rusia, China și Iranul rămân principalii actori care ar putea să interfereze cu alegerile din 2024, iar datorită progreselor tehnologice, alte națiuni sau chiar grupuri interne ar putea încerca să-și organizeze propriile campanii sofisticate de dezinformare. Cu toate acestea, Rusia rămâne „cea mai activă amenințare străină la adresa alegerilor", folosind mass-media de stat și influența online pentru a eroda încrederea în instituțiile democratice și în sprijinul SUA pentru Ucraina (AP,2024). Interferența Rusiei în viitoarele alegeri parlamentare din Uniunea Europeană ar putea pune în pericol procesul electoral, analizând astfel perioada alegerilor pentru data de 9 iunie 2024, nu au exista încercări majore de a influența opiniile electoratului pentru alegerile europene, chiar dacă au fost al doilea cel mai numeros proces electoral global după alegerile din India (The Record, 2024). Pentru alegerile europarlamentare din 9 iunie 2024 este posibil să fi existat incidente izolate de securitate cibernetică sau tentative de interferență cibernetică în diverse țări sau regiuni, dar acestea nu au fost raportate ca fiind de impact major în acea zi în Europa.

Un caz apărut în cadrul alegerilor este grupul de hacking numit R00Tk1t care a amenințat guvernul Indian pe canalul său de telegram că va ataca cibernetic și va manipula aparatele electronice de vot și a rezultatelor alegerilor. Grupul R00Tk1t este un actor proeminent al amenințărilor pe dark web, specializat în implementarea de software rău intenționat pentru a obține acces neautorizat la rețele sau sisteme, fără a lăsa urme de intruziune a acestora. Momentul acestui atac cibernetic asupra partidului Bharatiya Janata coincide cu alegerile din 2024 în India, care includ mai multe tipuri de alegeri. Acest proces electoral, care a avut loc între 19 aprilie 2024 și 1 iunie 2024, marchează cele mai mari alegeri din lume, cu noi implicații pentru viitorul guvernării indiene (The Cyber Express, 2024). Atacurile cibernetice asupra Indiei au fost identificate în timpul alegerilor, implicațiile au condus la scurgeri de date, dezinformare și spionaj cibernetic. De asemenea, pe forumurile Dark Web și pe Telegram au fost postate cărțile de identitate ale alegătorilor (Resecurity, 2024).

Utilizarea AI în cadrul alegerilor prezindenţiale este observată şi în China, unde sunt folosite conturi false de social media pentru a chestiona alegătorii în scopul influenţării alegerilor prezidenţiale din SUA, utilizând campanii de dezinformare cu ajutorul AI. Conturile actorilor afiliaţi Partidului Comunist Chinez sunt utilizate pentru a stoca date demografice chiar înainte de alegeri, utilizând inteligenţa artificială. Acest caz este primul identificat unde un stat foloseşte AI în încercarea de a influenţa alegeri externe. Gruparea Storm-1376 este unul dintre cele mai active grupări care a promovat o serie de imagini generate de inteligenţă artificială în cadrul alegerilor viitoare. Cu alegeri majore care au loc în întreaga lume anul acesta, în special în India, Coreea de Sud şi Statele Unite ale Americii, China va crea şi va amplifica, cel puţin, conţinut generat de inteligenţă artificială pentru a-şi urmării interesele geopoltice (Microsoft,2024).

Microsoft a declarat faptul că există campanii online provenite din Rusia care pot influenţa viitoarele alegeri prezidenţiale din SUA, acestea sunt identificate în ultimele 45 de zile, dar într-un ritm mai lent decât în alegerile trecute. Conturile legate de Rusia răspândesc conţinut care vizează publicul din SUA, criticând sprijinul american al Ucrainei în războiul acesteia cu Rusia. Deşi activitatea rusă nu este atât de intensă, aceasta ar putea creşte în lunile următoare. A fost observată o acţiune realizată de un grup rus de hacking numit Microsoft Star Blizzard, sau Cold River, care se concentrează pe ţintirea think tank-urilor occidentale. Acest grup vizează personalităţi politice şi cercurilor politice din SUA şi poate reprezenta un prim pas dintr-o serie de campanii de hacking (VOA, 2024).

Jocurile Olimpice de la Paris din 2024 pot reprezenta o nouă oportunitate pentru atacatorii cibernetici, deoarece pot afecta sportivii, participanţii şi infrastructura digitală. Atacurile cibernetice pot viza spionajul cibernetic, operaţiuni rău intenţionate, atacuri de phising, etc. cum au fost regăsite pentru prima data la jocurile olimpice de la Beijing din 2008. În anul 2012 a existat un atac major DDoS, ceea ce a dus noţiunea de ameninţare cibernetică pe agenda comunităţii olimpice. De asemenea, la jocurile olimpice de la Soci au existat ameninţări cibernetice asupra securităţii sistemelor IT, cât şi spionaj cibernetic, serviciile de securitate ruse colectând informaţii despre participanţi. La jocurile de la Rio, a fost regăsită implicarea serviciilor ruse prin GRU într-o campanie de spionaj cibernetic prin APT28. La jocurile olimpice din Coreea de Sud din 2018 au fost pertubate sistemele printr-un atac cibernetic major, prin viermele rău intenţionat numit „Olympic Destroyer”. La ultimele jocuri

olimpice din 2021 de la Tokyo, au fost înregistrate 450 de milioane amenințări cibernetice, cât și campanii de phishing. De asemenea, actorul de amenințări Sandworm APT asociat cu GRU a orchestrat o campanie de spionaj (SentinelOne, 2024).

Tensiunile geopolitice pot să influențeze Jocurile Olimpice, impactând în mod semnificativ atât dinamica evenimentului, cât și infractura trehnologică a acestuia. Aceste tensiuni pot de asemenea să amplice nevoia de a ataca acest eveniment pentru exploatarea vulnerabilităților și exfiltrarea datelor. Având în vedere faptul că Rusia între 2018-2022 a avut interdicție olimpică din cauza unui dopaj, implicarea ei în campanii rău intenționate poate să fie justificată deoarece în prezent are interdicție din cauza invaziei din Ucraina. Pe fondul sprijinului Franței pentru Ucraina în poziția sa defensivă împotriva Rusiei, există o posibilitate ca Jocurile Olimpice de la Paris din 2024 să devină o țintă pentru operațiunile cibernetice din Rusia și/sau Belarus (SentinelOne, 2024).

Concluzii și rezultatele obținute

Conceptul de cyber extortion asociat atacurilor ransomware este un subiect care a atras multă atenție în ultimii trei ani pentru cercetări. Ecosistemul criminalității cibernetice este unul complex, incluzând tipologii diferite de actori, roluri și acțiuni. În ultimul deceniu, ecosistemul cybercrime-as-a-service a evoluat și a adăugat noi provocări cu care se confruntă guvernele. Viitorul AI și rolul său în criminalitatea cibernetică poate fi privit din punct de vedere ofensiv. Conflictele globale pot să ducă la creșterea atacurilor cibernetice, cât și a criminalității cibernetice, utilizându-se tactici susținute de actori sponsorizați de stat sau de grupări neafiliate care operează în interes financiar.

Războiul cibernetic poate să reprezinte un instrument eficient pentru grupările de criminalitate cibernetică în atingerea obiectivelor politice, sociale sau naționale. Aceste obiective pot să aibă în vedere vizarea infrastructurii critice, furtul de date sensibile, dezinformarea, interese financiare etc. Exploatarea vulnerabilităților zero-day așa cum este situația grupări CL0P, poate reprezenta o escaladare în acest an.

Grupările de criminalitate cibernetică sunt importante de analizat în acest an, mai ales dacă vor apărea noi sesizări ale instituțiilor de securitate asupra serverelor acestora sau dacă își vor schimba tacticile sau vor acționa sub numele altui grup. Faptul că datele exfiltrate sunt stocate chiar dacă răscumpărarea este plătită, probabilitatea ca acele

date să fie folosite pentru a reextorca victimele este si mai mare şi va continua să crească.

Imprevizibilitatea executării atacurilor cibernetice poate să fie prezentă în anul 2024, deoarece peisajul ameninţărilor cibernetice este în continuă schimbare, derminată de integrarea accelerată a instrumentelor AI care a crescut substantial. În acest context este necesară colaborarea între guverne, organizaţii, instituţii etc în securitate cibernetică pentru a răspunde eficient ameninţărilor.

Colaborarea dintre criminalii cibernetici vorbitori de limbă engleză şi rusă pentru a lansa campanii de ransomware este o tendinţă notabilă pentru anul 2024. Adoptarea în masa a chatbot-urilor de inteligenţă artificială (AI) sub formă de modele de limbaj mari (LLM) la nivel global este regăsită începând cu 2023, iar în anii ce vor urma voi evoluat din ce în ce mai mult, având capacitatea de a manipula conţinutul online şi de a răspândi dezinformarea la un nivel şi cu o performanţă ridicată.

Analizând situaţiie din anii precedenţi, actorii de stat ostili din China, Rusia sau Coreea de Nord pot continua să lanseze campanii de intruziune mai avansate. Factorii geopolitici au jucat un rol semnificativ în modelarea securităţii informaţiilor. Conflictele dintre naţiuni precum Rusia şi Ucraina au influenţat tactica criminalilor cibernetici, iar atacurile ransomware au dat prioritate expunerii datelor şi cerând recompense ridicate.

În ceea ce privesc evenimentele din acest an, alegerile electorale de până acum au început să fie afectate, iar alegerile viitoare, mai ales cele prezidenţiale vor deveni ţinta mai multor atacuri cibernetice provenite din partea actorilor de criminalitate cibernetică sponsorizaţi de stat. Desi Jocurile Olimpice au devenit ţinte pentru operaţiuni cibernetice ofensive, cum ar fi: spionaj cibernetic, destabilizare sau câştig economic, viitoarele Jocuri de la Paris 2024 s-ar putea confrunta cu operaţiuni cibernetice mai variante şi mai persistente, variind de la campanii concentrate pe destabilizare, campanii de influenţă şi extorcare de date, până la cele centrate pe perturbări, inclusiv atacuri DDoS, phishing şi dezinformare.

Bibliografie:

1. "Businesses Ransomware Attack Rate Worldwide From 2017 to 2021." Statista. Accesat în data de 20 aprilie 2024. https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

2. AP News. 2024. "Facebook, TikTok Face Allegetions of Election Interference." Accesat în data de 16 mai 2024. https://apnews.com/article/election-interference-facebook-tiktok-russia-putin-china-1b5e5ce56d64dc356c2ad332068e2f8c

3. BankInfoSecurity. 2024. "Ransomware Operation LockBit Reestablishes Dark Web Leak Site." Accesat în data de 6 aprilie 2024. https://www.bankinfosecurity.com/ransomware-operation-lockbit-reestablishes-dark-web-leak-site-a-24442

4. Bitdefender. 2023. "Bitdefender Threat Debrief – December 2023." Accesat în data de 2 aprilie 2024. https://www.bitdefender.com/blog/businessinsights/bitdefender-threat-debrief-december-2023/

5. Bitdefender. 2024. "2024 Cybersecurity Forecast: Ransomware's News Tactics and Targets." Accesat în data de 21 martie 2024. https://www.bitdefender.com/blog/businessinsights/2024-cybersecurity-forecast-ransomwares-new-tactics-and-targets/

6. Bitdefender. 2024. "2024 Cybersecurity Predictions for AI: A Technical Deep Dive." Accesat în data de 26 martie 2024. https://www.bitdefender.com/blog/businessinsights/2024-cybersecurity-predictions-for-ai-a-technical-deep-dive/

7. Bitdefender. 2024. "2024 Cybersecurity Predictions: Changes in the Attack Landscape." Accesat în data de 13 aprilie 2024. https://www.bitdefender.com/blog/businessinsights/2024-cybersecurity-predictions-changes-in-the-attack-landscape/

8. Bitdefender. 2024. „Previziuni în securitate cibernetică pe 2024: Noi tactici şi ţinte vizate de ransomware." Softlead, Accesat la 19 aprilie 2024. https://softlead.ro/noutati-it-c/bitdefender-previziuni-in-securitate-cibernetica-pe-2024-noi-tactici-si-tinte-vizate-de-ransomware.html

9. Bushido Token Blog. 2024. "Top 10 Cyber Threats of 2023." Accesat în data de 14 aprilie 2024. https://blog.bushidotoken.net/2023/12/top-10-cyber-threats-of-2023.html

10. Cloudflare. 2024. "What is a Large Language Model?" Accesat în data de 28 martie 2024. https://www.cloudflare.com/learning/ai/what-is-large-language-model/

11. European Union Agency for Cybersecurity (ENISA). 2023. Enisa Threat Landscape 2023. Accesat în data de 18 martie 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

12. Microsoft. 2024. "China, AI Influence Elections, MTAC Cybersecurity." Accesat în data de 8 aprilie 2024. https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/

13. Ransomware Sommelier. 2024. "Ransomware Attacks Against Local Authorities." Accesat în data de 30 martie 2024. https://ransomwaresommelier.com/p/ransomware-attacks-against-local

14. Recorded Future Blog. 2024. "Improving Dark Web Investigations with Threat Intelligence." Accesat în data de 19 aprilie 2024. https://www.recordedfuture.com/blog/improving-dark-web-investigations-with-threat-intelligence

15. Resecurity. 2024 "Cybercriminals Are Targeting Elections in India with Influence Campaigns." Accesat în data de 22 mai, 2023. https://www.resecurity.com/blog/article/cybercriminals-are-targeting-elections-in-india-with-influence-campaigns

16. SC Magazine. 2023. "Report: Ransomware Payouts and Recovery Costs Went Way Up in 2023." Accesat în data de 24 martie 2024. https://www.scmagazine.com/resource/report-ransomware-payouts-and-recovery- costs-went-way-up-in-2023

17. SentinelOne Blog. 2024. "Integrating ChatGPT Generative AI Within Cybersecurity Best Practices." Accesat în data de 20 aprilie 2024. https://www.sentinelone.com/blog/integrating-chatgpt-generative-ai-within-cybersecurity-best-practices/

18. SentinelOne Blog. 2024. "Ransomware Evolution: How Cheated Affiliates are Recycling Victim Data for Profit." Accesat în data de 25 aprilie 2024. https://www.sentinelone.com/blog/ransomware-evolution-how-cheated-affiliates-are-recycling-victim-data-for-profit/

19. SentinelOne. 2023. "Endpoint. Identity, and Cloud: Top Cyber Attacks of 2023 So Far." Accesat în data de 20 martie 2024. https://www.sentinelone.com/blog/endpoint-identity-and-cloud-top-cyber-attacks-of-2023-so-far/

20. SentinelOne. 2024. "Cybersecurity at the 2024 Paris Summer Olympics: Safeguarding the Spectacle." Accesat în data de 12 aprilie 2024. https://www.sentinelone.com/blog/cybersecurity-at-the-2024-paris-summer-olympics-safeguarding-the-spectacle/

21. SOCRadar. 2024. "Dark Web Profile: Red Ransomware." Accesat în data de 25 aprilie 2024. https://socradar.io/dark-web-profile-red-ransomware/

22. SOCRadar. 2024. "Top 5 Russian-Speaking Dark Web Forums." Accesat în data de 21 martie 2024. https://socradar.io/top-5-russian-speaking-dark-web-forums/

23. The Hacker News. 2024. "Cyber Threat Landscape: 7 Key Findings." Accesat în data de 3 aprilie 2024. https://thehackernews.com/2024/01/cyber-threat-landscape-7-key-findings.html

24. The Hacker News. 2024. "Cybersecurity Tactics FinServ Institutions Can Bank On in 2024." Accesat în data de 18 aprilie 2024. https://thehackernews.com/2024/02/cybersecurity-tactics-finserv.html

25. The Hacker News. 2024. "LockBit Ransomware Operation Shut Down." Accesat în data de 5 aprilie 2024. https://thehackernews.com/2024/02/lockbit-ransomware-operation-shut-down.html

26. The Hacker News. 2024. "Microsoft, OpenAI Warn of Nation-State Hackers Weaponizing AI for Cyber Attacks". Accesat în data de 16 aprilie 2024. https://thehackernews.com/2024/02/microsoft-openai-warn-of-nation-state.html

27. The Hacker News. 2024. "Ransomware Double-Dip: Re-Victimization in Cyber Extortion." Accesat în data de 22 aprilie 2024. https://thehackernews.com/2024/04/ransomware-double-dip-re-victimization.html

28. The Record. 2024. "Russian Interference in European Elections a Clear Threat: Margaritis Schinas." Accesat în data de 10 aprilie 2024. https://therecord.media/russian-interference-european-elections-clear-threat-margaritis-schinas

29. Trend Micro. 2024. "LockBit Attempts to Stay Afloat with a News Version." Accesat în data de 8 aprilie 2024. https://www.trendmicro.com/en_no/research/24/b/lockbit-attempts-to-stay-afloat-with-a-new-version.html

30. University Oxford. 2024. "World First Cybercrime Index Ranks Countries' Cybercrime Threat Level." Accesat în data de 21 aprilie 2024. https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level

31. VOA News, 2024. "Microsoft Finds Russian Influence Operations Targeting US Election Have Begun." Accesat în data de 17 aprilie 2024. https://www.voanews.com/a/microsoft-finds-russian-influence-operations-targeting-us-election-have-begun-/7574036.html

Aceasta este al treilea volum de proceedings al Conferinței Științifice Intelligence și Cultura de Securitate (ICS), care cuprinde lucrările prezentate în cadrul ediției din 2024 - ICS 2024, 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 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