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

Analizë teknike për skedarin keqdashës

Dokumenti përmban përmbajtje që shkel të drejtat e autorit.zip

Versioni: 1.0
Datë: 29/09/2025

PËRMBAJTJA

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 që shënjestron infrastrukturat kritike dhe të rëndësishme të Republikës së Shqipërisë, ku në përmbajtjen e email phishing ndodhet një skedar bashkëlidhur me emërtimin ***Dokumenti përmban përmbajtje që shkel të drejtat e autorit.zip***. Ky skedar ka si qëllim të kryejë komandim në distancë nga aktorët keqdashës drejt kompjuterave apo sistemeve të viktimave.

Dokumenti përmban përmbajtje që shkel të drejtat e autorit.zip

Analiza e këtij skedari fillon me ekstraktimin nga formati .zip (i arkivuar). Skedari i parë që evidentohet është ***Dokumenti përmban përmbajtje që shkel të drejtat e autorit.exe*** i cili është një skedar i tipit ***PE(Portable Executable***), skedar i ekzekutueshëm. Gjithashtu nëse kemi opsionin "**View hidden items**" në Windows evidentohen dhe disa skedarë të tjerë të fshehur.

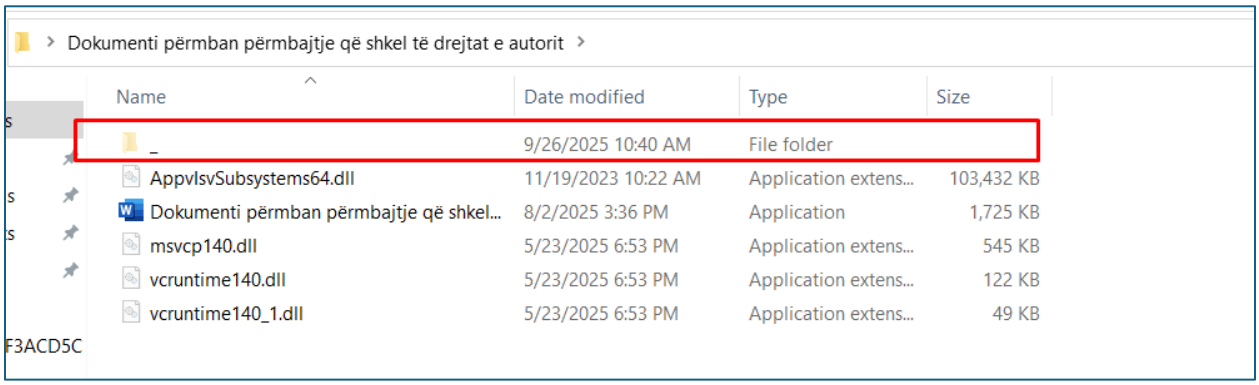


Figura 1.Skedarët e fshehur.

Këtu evidentohet edhe skedari më i rëndësishëm i zinxhirit të infektimit qe është ***dynamic link library "AppvIsvSubsystems64.dll"*** i cili ka një madhësi **~103 mb** ku paraqitet një element që nuk është shumë i zakonshëm. Gjatë analizës statike evidentohen funksione që bëjnë kontrollin e direktorive, pra ky skedar ***dll*** fillon të kërkojë për vendndodhjet e skedarëve të ndryshëm. Por për të parë se çfarë funksioni thirret konkretisht, kryhet procesi i ***debug***.

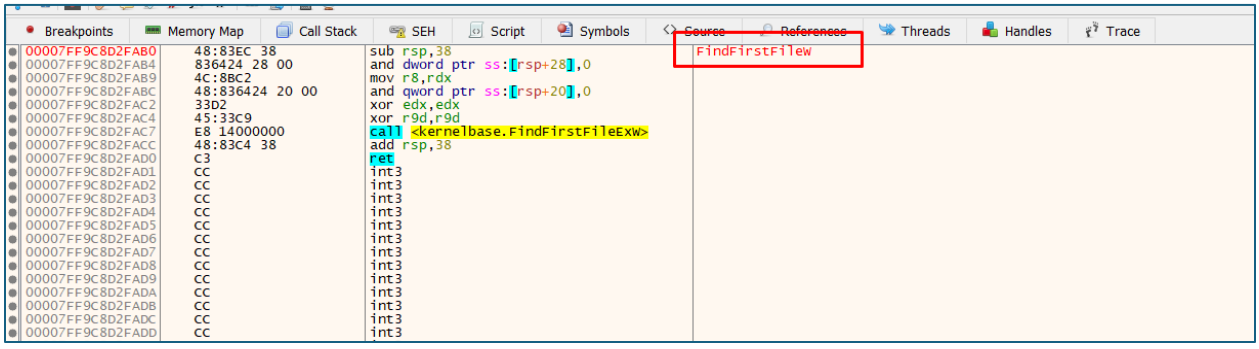


Figura 2.Funksioni FindFirstFileW.

Gjatë **debug** të skedarit dll, në regjistrin **RDX** në memorjen ***dump*** evidentohet kontrolli i folderit **"_"** nga ku evidentohet se kjo direktori përmban ***payload*** për të vazhduar qëllimin kryesor të skedarit.

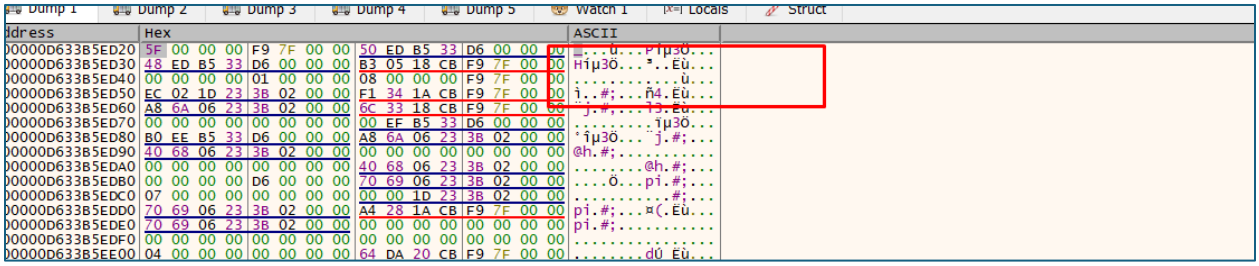


Figura 3. Kontrolli i direktorisë "_".

Direktoria "_" përmban disa skedarë nga të cilët disa janë ***PDF*** legjitime por ka dhe skedarë të tjerë të cilët duket sikur janë të pa aksesueshëm por mund të dekodohen në një fazë tjetër dhe përdoren për qëllime të tjera.

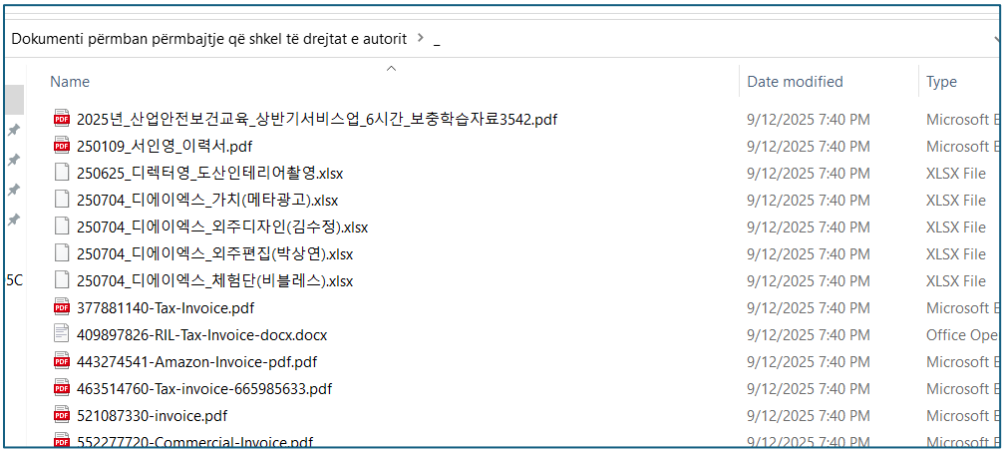


Figura 4.Përmbajtja e direktorisë "_".

Skedari më kryesor në këtë direktori është skedari **Images.png** i cili pavarsisht prapashtesës që ka, nuk është një imazh por është aplikacioni i arkivimit **WinRar,** i cili aksesohet nëpërmjet ***cmd*** me komandën:

images.png x -ibck -y -paFr25vHl9vULPjJoV8rUcLS6YCzbMQ8k Invoice.pdf C:\\Users\\Public

Winrar në këtë rast ekstrakton në direktorinë **C:\Users\Public** një direktori e cila në vetvete është **libraria** e **Python**.

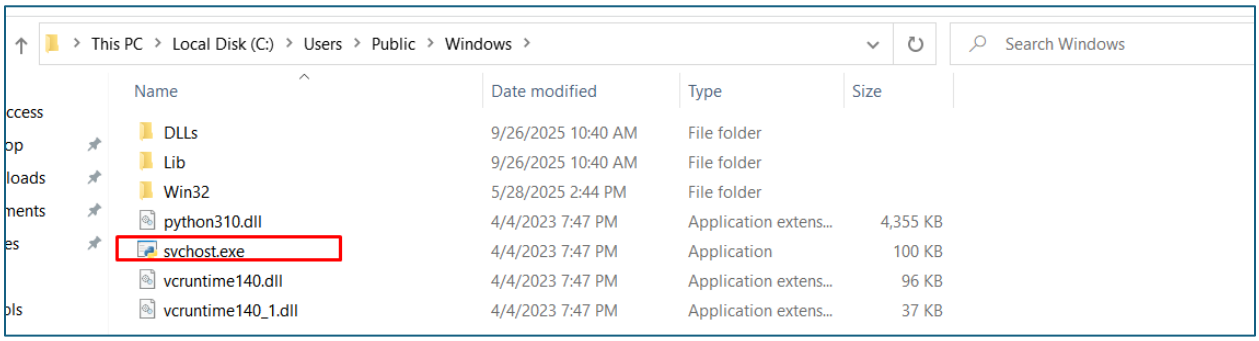


Figura 5. Python.exe i kamufluar si svchost.exe.

Svchost.exe apo **python.exe** në këtë rast nuk është keqdashës, por duke parë logjikën e funksionimit të këtij skedari keqdashës deri tani, python duhet të marrë ndonjë parametër në mënyrë që të shkoj në fazën finale të tij. Gjatë kërkimit në **C:\Users\Public\Windows\Lib** u evidentua një skedar përsëri i dyshimtë me

emrin **images.png**, i përsëritur si në rastin më parë.

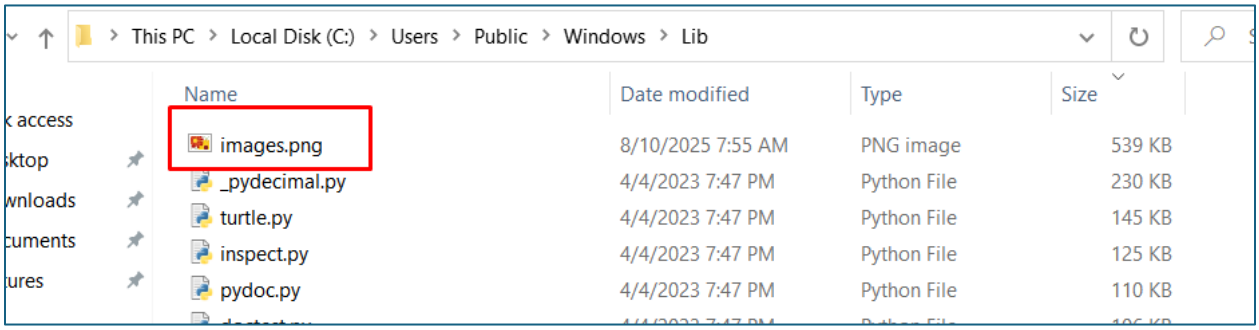


Figura 6. images.png faza e 2.

Ky skedar është i tipit ***.py*** pavarsisht prapashtesës së tij. Nga analiza në një editues teksti të zakonshëm nxirret dhe kodi i tij si më poshtë vijon:

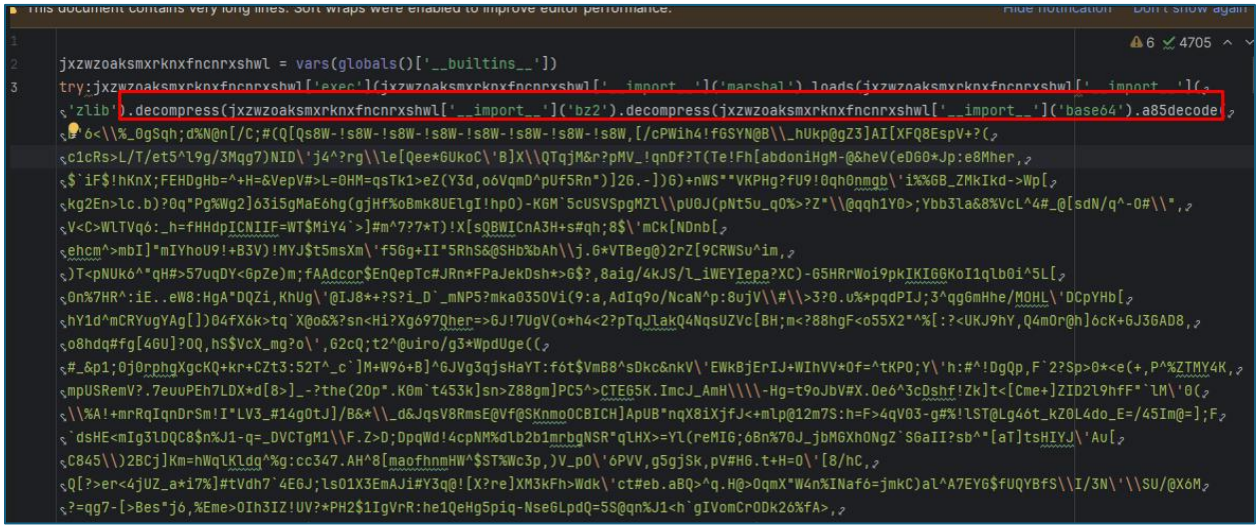


Figura 7. Kodi i images.png.

Kjo pjesë kodi është e fshehur dhe e përdorur për të kryer qëllimin e vërtetë të skedarit. Më tej,krijohet një variabël me emrin **xzwzoaksmxrknxfncnrxshwl** që përdoret për të thirrur funksionet bazë të **python**. Brenda bllokut **try** evidentohen këto funksione kryesore:

__import__('base64').a85decode(...) nga ku :

- Importon librarianë **base64** dhe përdor funksionin **a85decode**.
- **a85decode** shërben për të dekoduar tekst të koduar në format **Ascii85/Base85**.

Rezultati i këtij dekodimi dërgohet tek **__import__('bz2').decompress(...)**

- Pra, të dhënat e dekoduara kalojnë përmes **BZ2 decompress** (ekstraktim nga algoritmi Bzip2).

Më pas, rezultati kalon në **__import__('zlib').decompress(...) :**

- Këtu ekstraktohet edhe një herë duke përdorur algoritmin **zlib**.

marshal.loads(...).

- **marshal** përdoret për të deserializuar objekte **Python**. Këtu pritet që rezultati i dekompresimeve të jetë **një kod (code object)** të serializuar **(p.sh. një .pyc-like object).**

exec(...)

- Në fund, **exec** ekzekuton objektin e krijuar (ose përmbajtjen e ***de-marshal***). Pra kodi që ishte fshehur do të ekzekutohet në ambientin aktual.

Po të modifikojmë kodin hap pas hapi kuptojmë sjelljen e tij për çdo funksion specific.

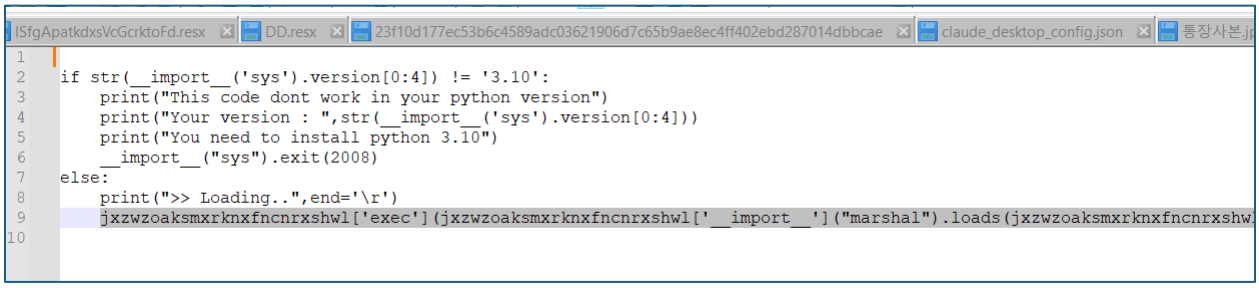


Figura 8. Dekodimi i fazës së parë të scriptit.

Ajo çfarë e bën interesante është kushti logjikë ***if*** që tregon se versioni që duhet për këtë skedar të funksionojë është versioni **3.10.**
Në **else** vazhdon përsëri e njëjta logjikë si më parë dhe përsëri nëse modifikohet kodi deri sa të arrihet në fazën finale ***dissasemble*** i objektit **pyc** dhe aksesimi i kodit real.

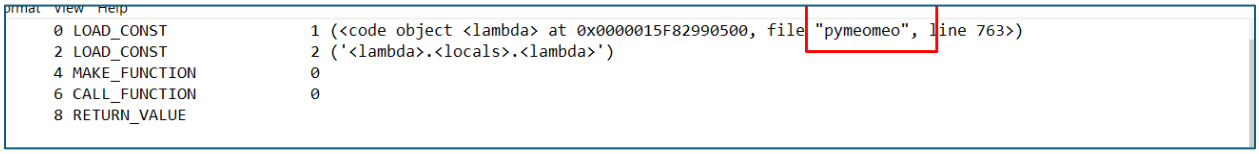


Figura 9. String pymeomeo.

Gjatë **disassemble** të objekteve **pyc,** evidentohet vargu i karaktereve **pymeomeo** i cili,nëse kërkohet informacion global për të kuptohet se për fshehjen e kodit është përdorur:

- https://github.com/zrsx/PYMEOMEO

"**Advanced Python Obfuscation and Protection Suite".** Kjo vërtetohet dhe nga skedarët që janë në *github* ku fshehja e kodit bëhet në varësi të versionit të python të instaluar,fakt i cili është evidentuar më parë gjatë analizës. Nëse krijohet një skedar i thjeshtë python me tekstin **"Hello World"** dhe fshihet me këtë projekt rezultati i kodit do jetë i njëjtë me kodin e python të **images.png.**

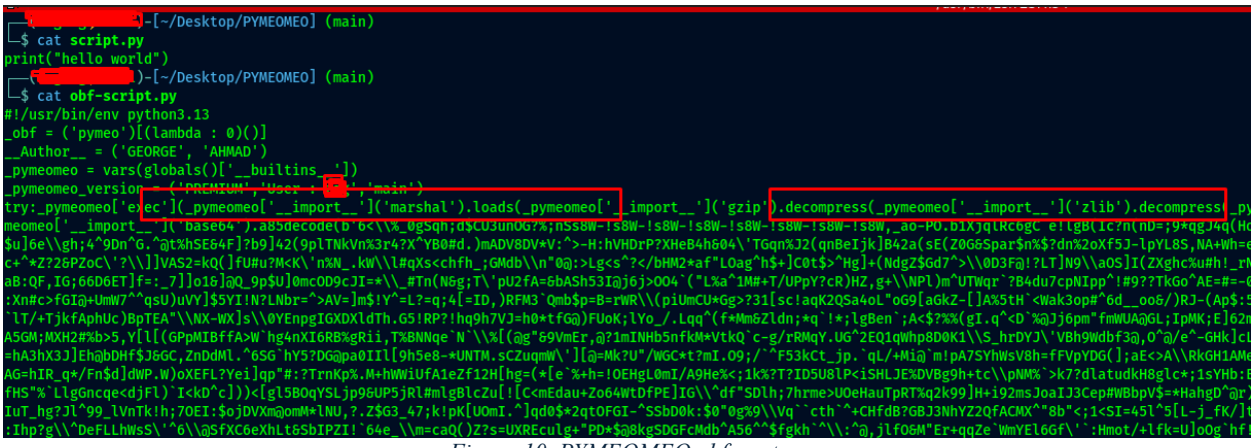


Figura 10. PYMEOMEO obfuscator.

Gjatë procesit *disassembly*, evidentohet dhe një shtresë tjetër fshehjeje duke shfaqur karakteret në vargje të enkoduara.

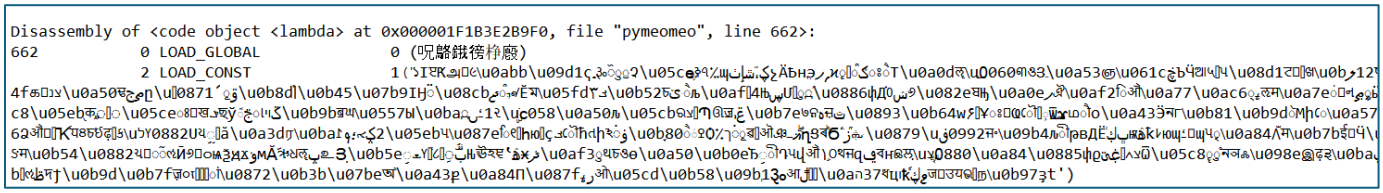
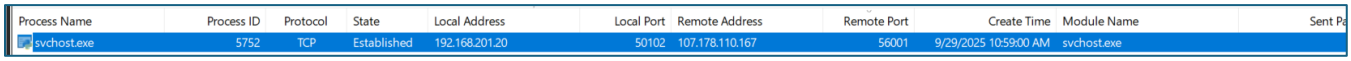


Figura 11. Kodi i enkoduar.

Duke parë nivelin e fshehjes që paraqitet shumë i lartë, kontrollohen se çfarë aktiviteti dinamik kryen skedari keqdashës me parametrin e **images.png.** Nga kjo rezulton se aktorët keqdashës arrijnë të kryejnë komandim në distance dhe më tej sipas interesave të kryejnë veprime të tjera jo legjitime. Në fund të zinxhirit ky skedar i ekzekutueshëm realizon një komunikim me serverin C2 me ip: **107[.]178[.]110[.]167**



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Pa
svchost.exe	5752	TCP	Established	192.168.201.20	50102	107.178.110.167	56001	9/29/2025 10:59:00 AM	svchost.exe	

Figura 12. IP Command And Control.

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	Valid Accounts	1 Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	4 1 1 Process Injection	1 1 Masquerading	1 OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Email Collection	2 Encrypted Channel	Exfiltration Over Other Network Medium	1 Data Encrypted for Impact
Credentials	Domains	Default Accounts	1 Command and Scripting Interpreter	1 DLL Side-Loading	1 Abuse Elevation Control Mechanism	1 Disable or Modify Tools	LSASS Memory	1 Query Registry	Remote Desktop Protocol	2 Data from Local System	1 Remote Access Software	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	4 1 1 Process Injection	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	1 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	1 DLL Side-Loading	1 Abuse Elevation Control Mechanism	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	2 Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 Rundll32	LSA Secrets	1 4 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 DLL Side-Loading	Cached Domain Credentials	Wi-Fi Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop

Indikatorët e Kompromitimit

Dokumenti përmban përmbajtje që shkel të drejtat e autorit.exe	**341BA8A556F4AC503AB23D9E5D2114261AFD24AED332F2E404705B522AFD5998**
AppvIsvSubsystems64.dll	**653F1B0F2B4C711B46016C268FB985D82528BB4240E202BE9640F31A0E6217B8**
Images.png	**A5B19195F61925EDE76254AAAD942E978464E93C7922ED6F064FAB5AAD901EFC**

C2	**107[.]178[.]110[.]167**

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 kritike 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 sjelljeje (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".