PHISHING?

in questa dimostrazione vedremo l’analisi di un link -REALE MALEVOLO- col quale sono entrato in contatto tramite condivisione da account rubati.

01 Leonardo Sanzone

SEGNALAZIONE

Stavo trascorrendo il mio tempo a cercare il più possibile di far del male alla mia Flare VM, quando ad un tratto mi sono imbattuto in questo link:

steam gift 50$ - steamcommunity.com/gift-card/pay/50

Nonostante il mio animo nerd si stesse già strofinando le mani, ho deciso di esaminare meglio questo link per capire cosa si potesse celare dietro di esso.

```
1<@932766035105439774> steam gift 50$ - [steamcommunity.com/gift-card/pay/50](https://is.gd/9Xf04G )
```

E’ già bastato leggere il testo originale per rendersi conto che il vero link, al quale sarei stato rimandato, non era quello che invece mi era stato fatto credere.

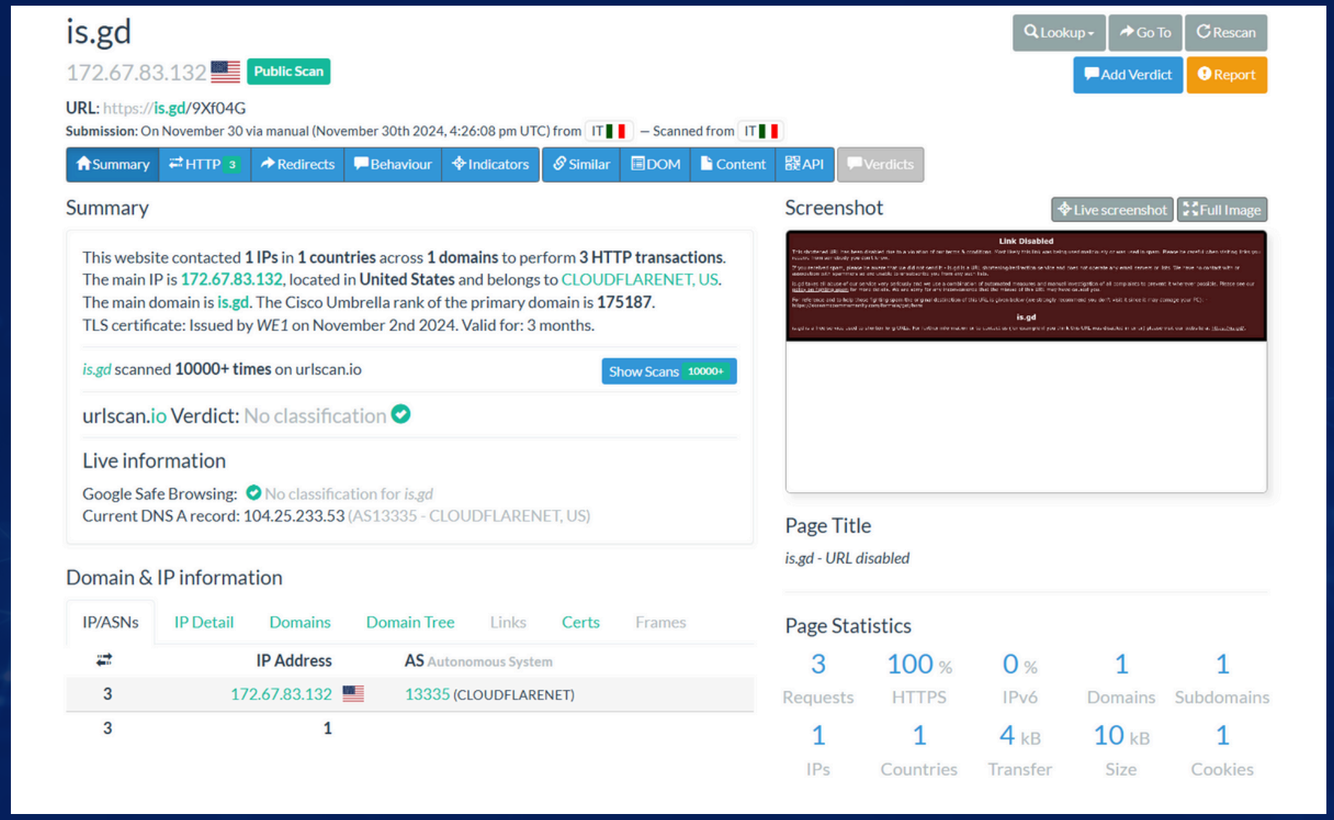
VISION AND MISSION

```
(https://is.gd/9Xf04G )
```

Di fatto il link reale è quello evidenziato alla fine, ed è da qui che, tramite dei primi indizi, la mia ricerca inizierà.

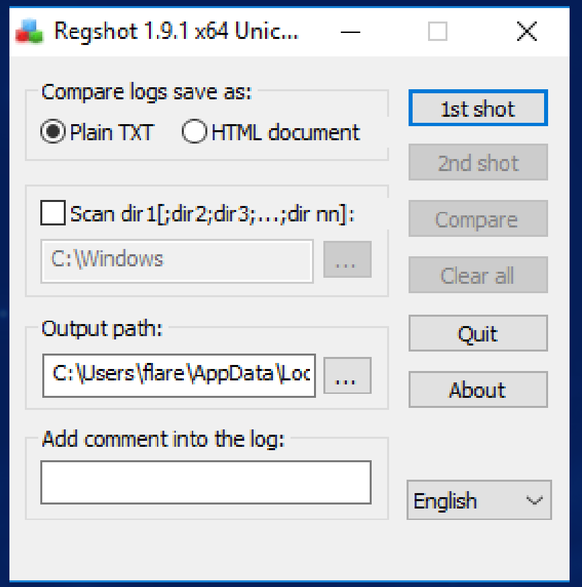
URLSCAN

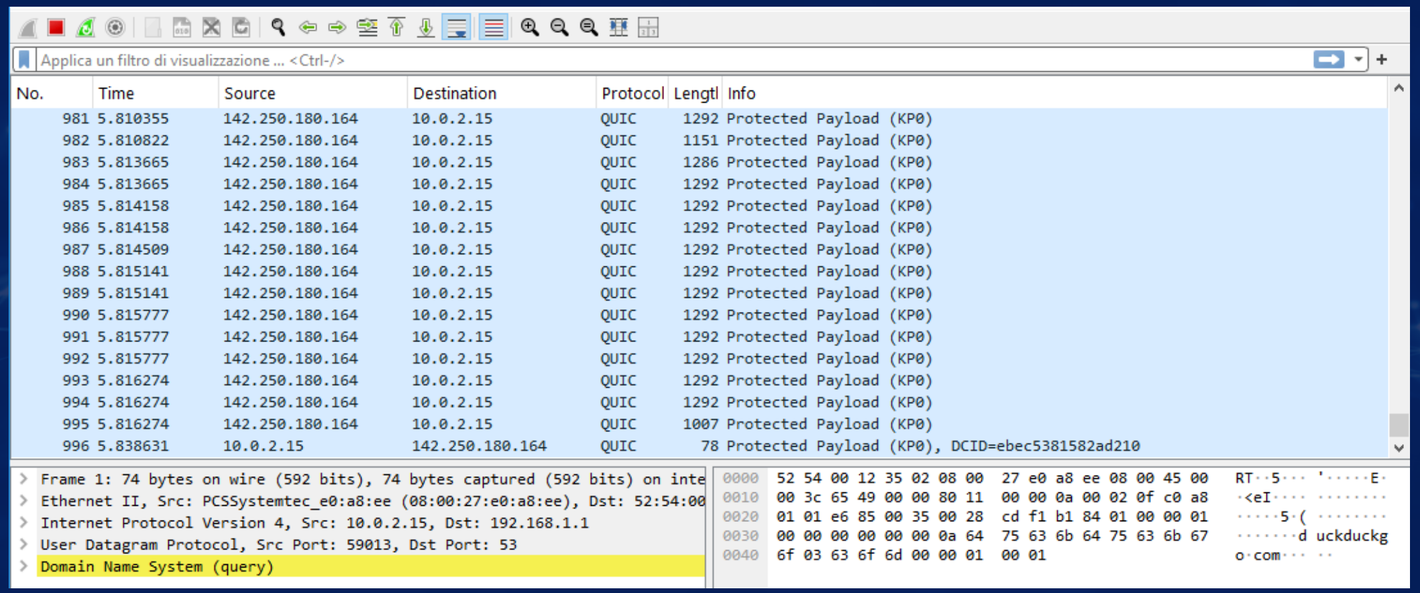
Tramite una ricerca su URLscan notiamo come is.gd sia un servizio usato per accorciare gli URL, in molti casi usato per mascherare email di phishing.

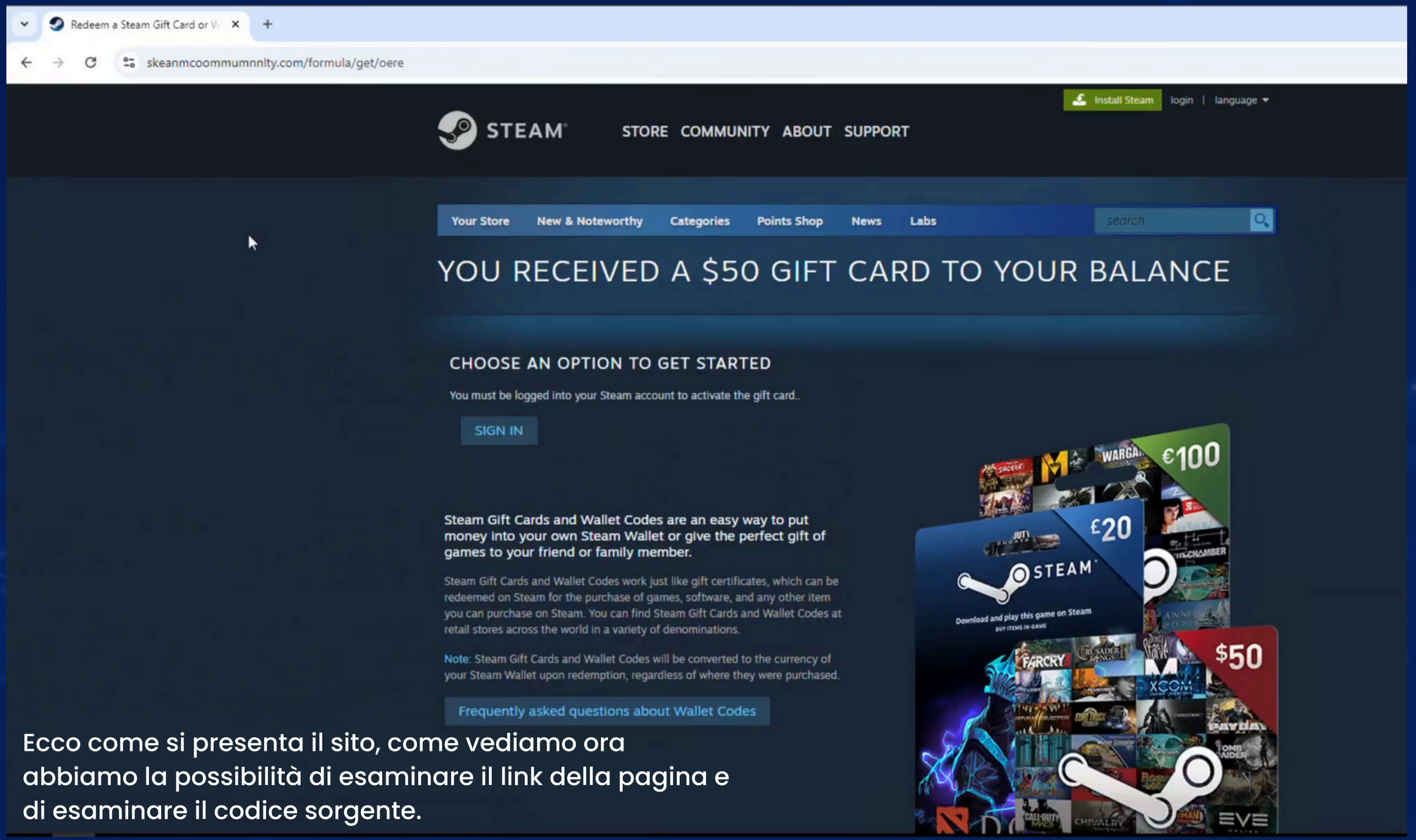


- Svolgerò la seguente analisi attraverso la mia macchina virtuale Flare, appositamente settata e pensata per effettuare test di svariate tipologie senza rischio per l'OS principale.

- Come primo procedimento attivo subito "Regshot", per tenere traccia di eventuali rilevanti variazioni nelle mie chiavi di registro e mi preoccupo di mettere in ascolto "Wireshark" per rintracciare connessioni sospette.





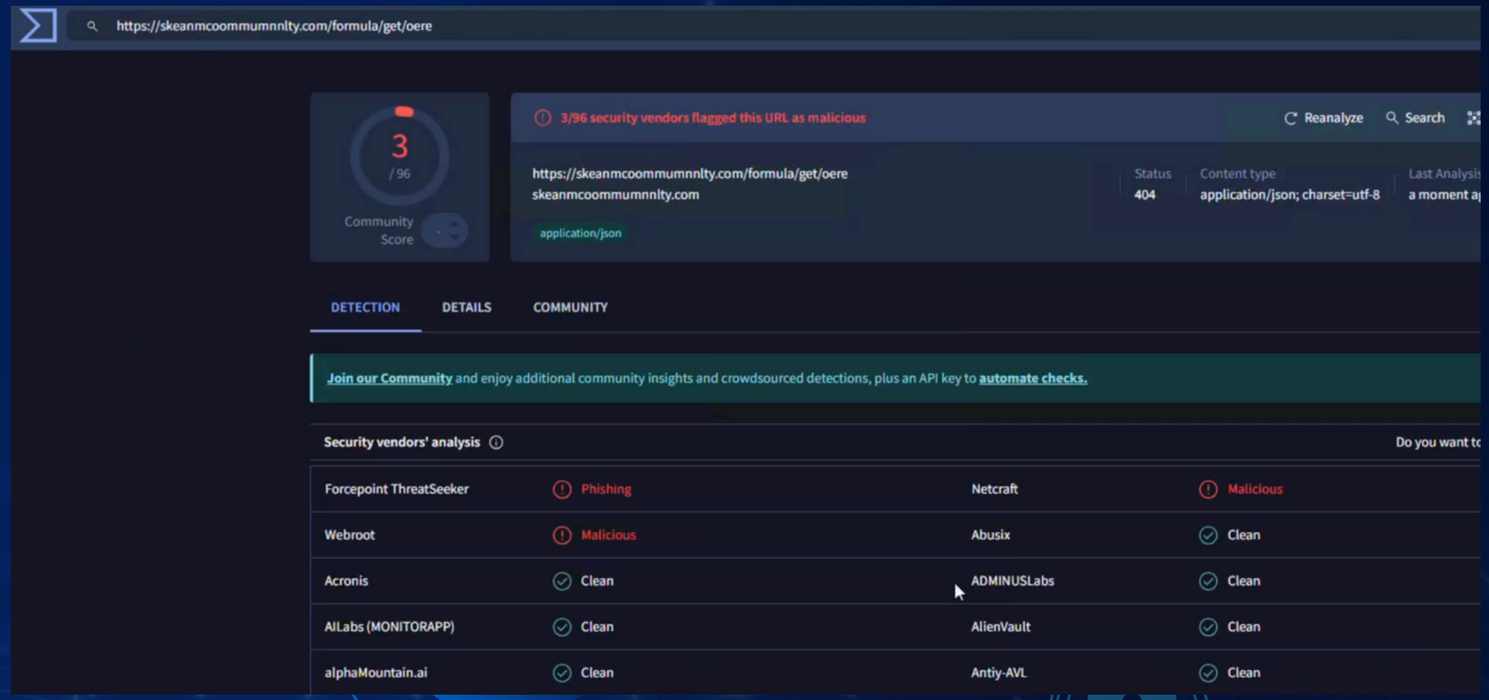


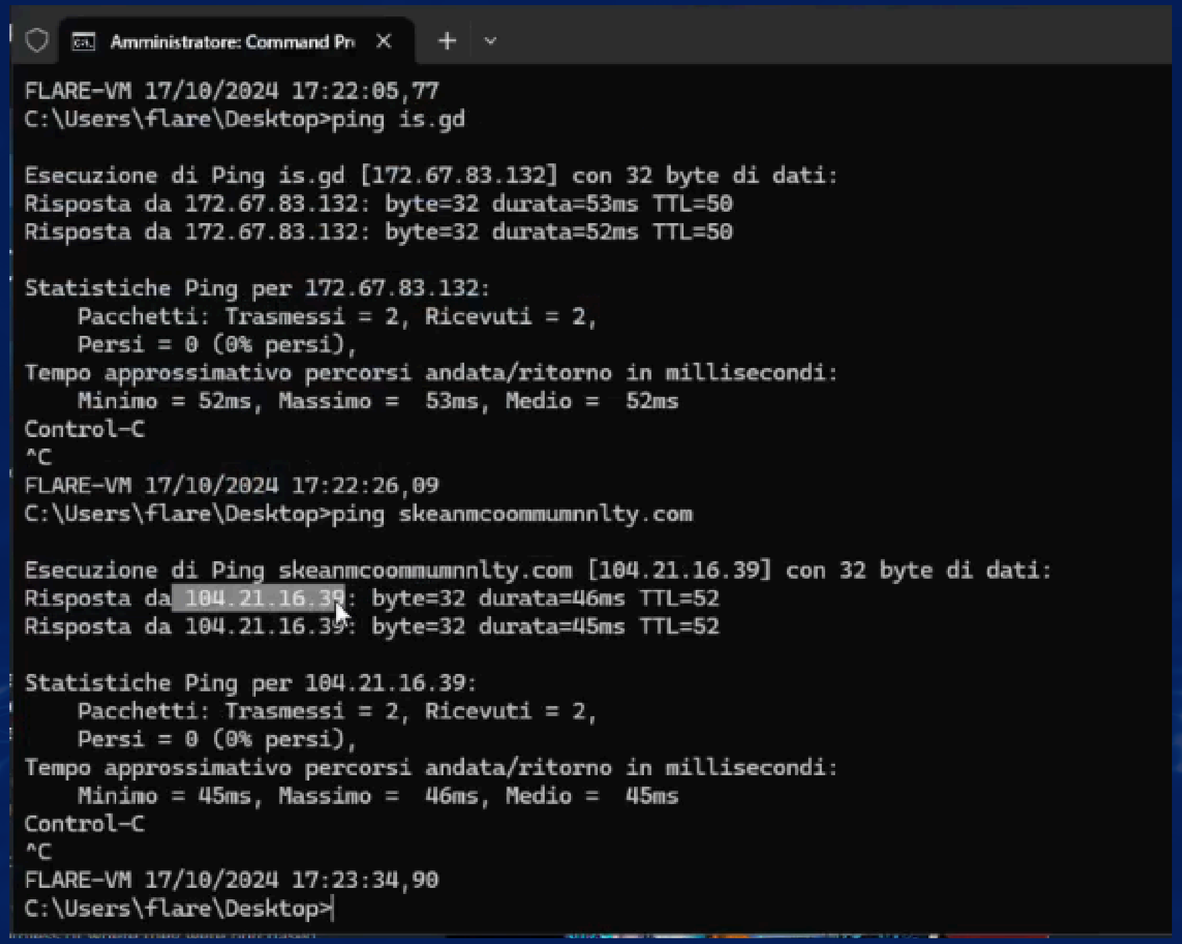
Ecco come si presenta il sito, come vediamo ora abbiamo la possibilità di esaminare il link della pagina e di esaminare il codice sorgente.

VIRUSTOTAL

Analizziamo il nuovo link

Come ulteriore conferma, VirusTotal, a gran fatica, ci fa notare come questo link potrebbe, secondo pochi antivirus, essere malevolo.



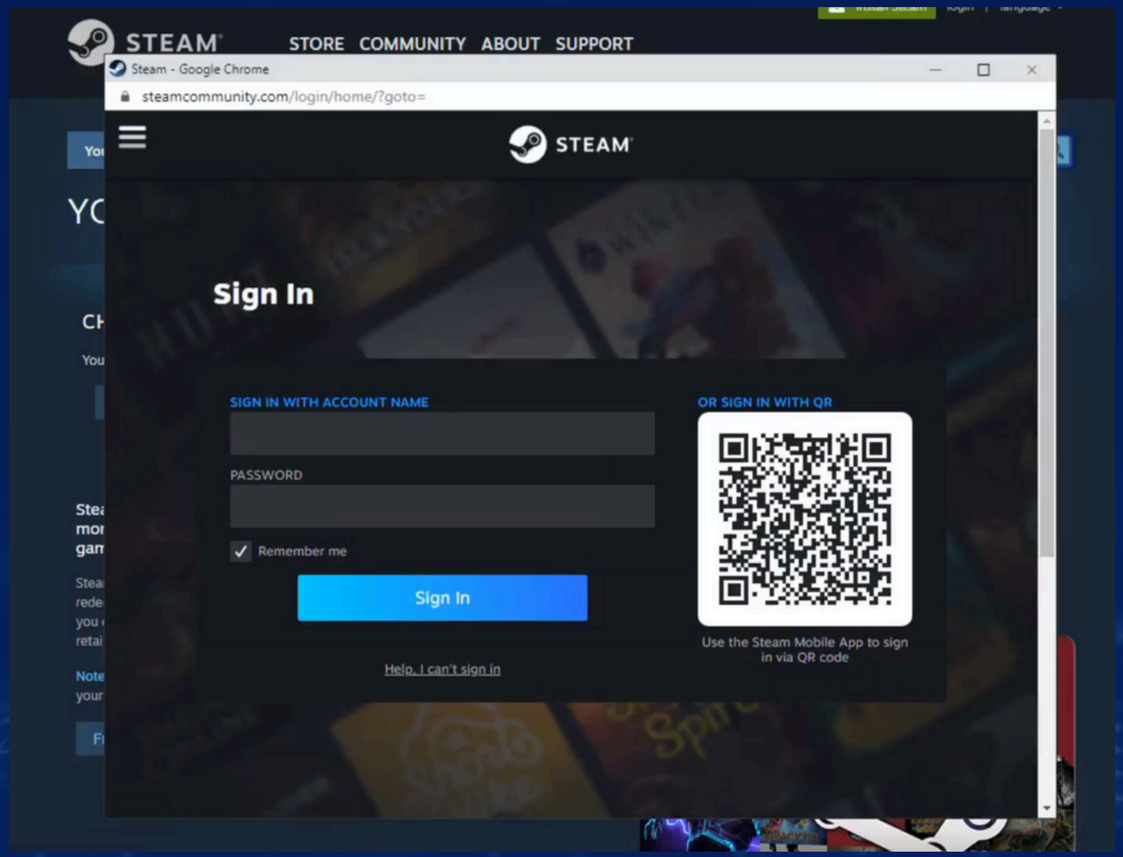


RINTRACCIAMO GLI IP

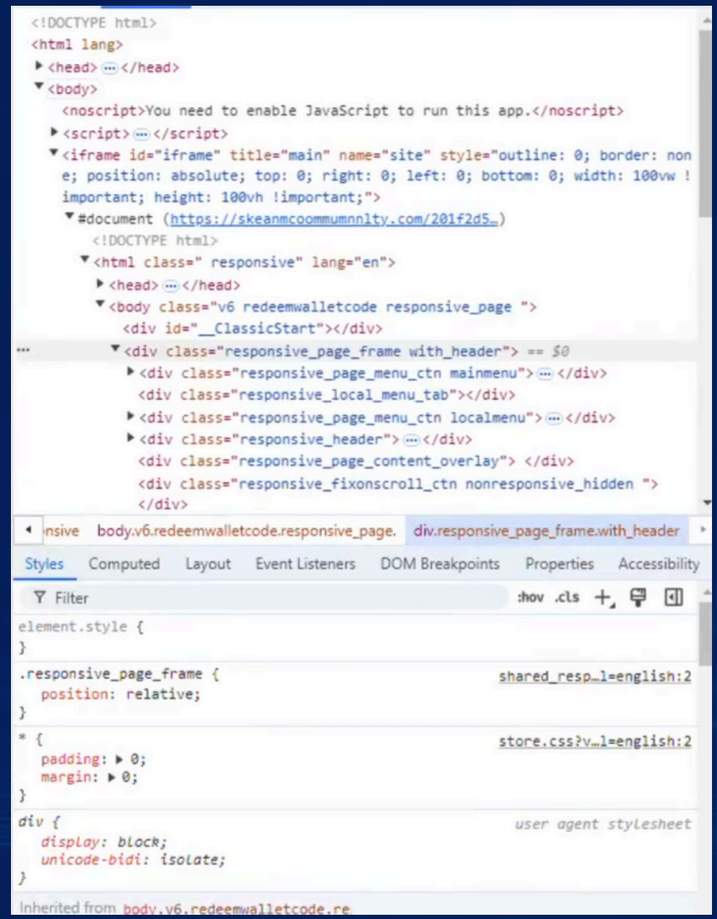
Tramite ping ci è possibile rintracciare gli indirizzi IP, i quali ci serviranno per una eventuale approfondita analisi tramite Wireshark.

Notiamo infatti come il primo questi IP sia quello che abbiamo rintracciato tramite URLscan a seguito del ping di is.gd.

Per quanto riguarda il secondo, quest'ultimo IP risulta essere associato al link trovato una volta entrati all'interno della pagina.



A seguito di una analisi del codice tramite VirtualStudio code, sono arrivato alla conclusione che la pagina presentata sia effettivamente quella ufficiale del sito di steam.

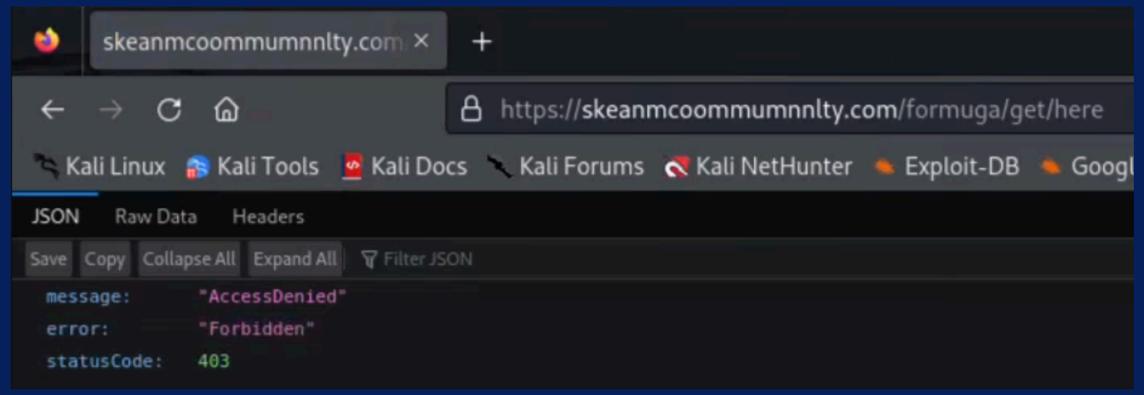


E’ però interessante notare come l’attaccante abbia ideato un iframe che reindirizzi la vittima, qualsiasi sia l’interazione che essa abbia con la pagina, ad una seconda pagina con lo scopo di prelevare le credenziali e mandarle al nostro malintenzionato.

```
-----------------------------------
Keys added: 59
-----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Mrt
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Mrt\_Merged
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Mrt\_Merged\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2408
HKLM\SYSTEM\Software\Microsoft\TIP\TestResults
HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.html
HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.html\OpenWithList
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000020368
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000020382
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000050392
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000000503E2
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000C02B2
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\CIDOpen
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\CIDOpen\Modules
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\CIDOpen\Modules\GlobalSettings
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\CIDOpen\Modules\GlobalSettings\ProperTreeModuleInner
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012024100720241014
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012024101720241018
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Microsoft\Windows\CurrentVersion\Search\JumplistData
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Microsoft\ActiveMovie
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Microsoft\ActiveMovie\devenum 64-bit
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\0
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\0\0
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\5
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\19\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\4\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\20
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\20\ComDlg
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\20\ComDlg\{CD0FC69B-71E2-46E5-9690-5BCD9F57AAB3}
```

Terminata la ricerca, sono felice di notare che non ci siano state particolari modifiche alle mie chiavi di registro, posso quindi immaginare che nessun Malware sia entrato nella mia VM tramite il sito, o che comunque, in caso sia successo, ancora non sia stato messo in funzione.

ALTRO RIGUARDO ALL'ANALISI



Il sito non mi fa accedere tramite la mia Kali, credo che visto che quest'ultima è estremamente protetta, il sito si difenda per non farsi scoprire da eventuali Antivirus o sistemi di sicurezza.

Dopo essere tornato, successivamente, per effettuare ulteriori ricerche, il sito era stato chiuso per attività Malevola.