



PHISHING?

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



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.

(<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.

VISION AND MISSION





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.

is.gd

172.67.83.132 Public Scan

URL: <https://is.gd/9Xf04G>

Submission: On November 30 via manual (November 30th 2024, 4:26:08 pm UTC) from – Scanned from

Summary HTTP 3 Redirects Behaviour Indicators Similar DOM Content API Verdicts

Summary

This website contacted 1 IPs in 1 countries across 1 domains to perform 3 HTTP transactions. The main IP is [172.67.83.132](#), located in [United States](#) and belongs to [CLOUDFLARENET, US](#). The main domain is [is.gd](#). The Cisco Umbrella rank of the primary domain is [175187](#). TLS certificate: Issued by [WE1](#) on November 2nd 2024. Valid for: 3 months.

[is.gd](#) scanned 10000+ times on urlscan.io [Show Scans 10000+](#)

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for [is.gd](#)
Current DNS A record: 104.25.233.53 (AS13335 - CLOUDFLARENET, US)

Domain & IP information

IP/ASNs	IP Detail	Domains	Domain Tree	Links	Certs	Frames
3	IP Address 172.67.83.132	13335 (CLOUDFLARENET)				
3		1				

Page Statistics

3	100 %	0 %	1	1
Requests	HTTPS	IPv6	Domains	Subdomains
1	1	4 kB	10 kB	1
IPs	Countries	Transfer	Size	Cookies



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.

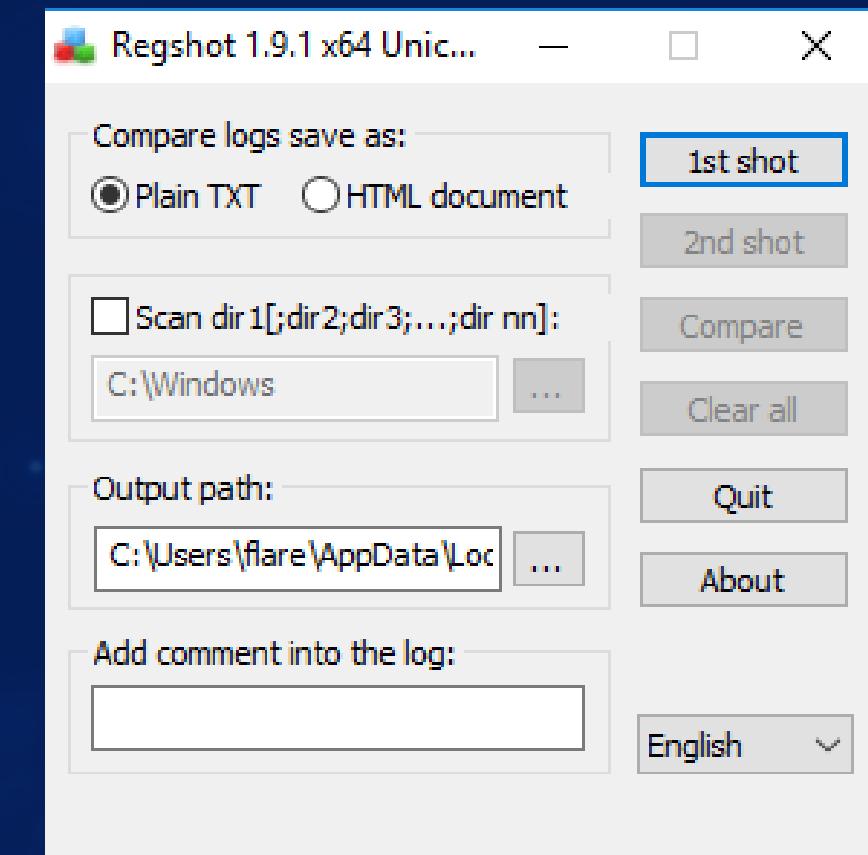


Come primo procedimento attivo subito "Regshot", per tenere traccia di eventuali rilevanti variazioni nelle mie chiavi di registro e mi preoccupo di mettere in ascolto "Wireshark" per rintracciare connessioni sospette.

The screenshot shows the Wireshark interface with a list of captured frames. The columns include No., Time, Source, Destination, Protocol, Length, and Info. Frame 981 is selected, showing details: Source 142.250.180.164, Destination 10.0.2.15, Protocol QUIC, Length 1292, and Info Protected Payload (KP0). The Info column also displays the full hex and ASCII dump of the frame. A yellow highlight covers the bottom section of the frame details, which includes a list of protocol headers and their values.

No.	Time	Source	Destination	Protocol	Length	Info
981	5.810355	142.250.180.164	10.0.2.15	QUIC	1292	Protected Payload (KP0)
982	5.810822	142.250.180.164	10.0.2.15	QUIC	1151	Protected Payload (KP0)
983	5.813665	142.250.180.164	10.0.2.15	QUIC	1286	Protected Payload (KP0)
984	5.813665	142.250.180.164	10.0.2.15	QUIC	1292	Protected Payload (KP0)
985	5.814158	142.250.180.164	10.0.2.15	QUIC	1292	Protected Payload (KP0)
986	5.814158	142.250.180.164	10.0.2.15	QUIC	1292	Protected Payload (KP0)
987	5.814509	142.250.180.164	10.0.2.15	QUIC	1292	Protected Payload (KP0)
988	5.815141	142.250.180.164	10.0.2.15	QUIC	1292	Protected Payload (KP0)
989	5.815141	142.250.180.164	10.0.2.15	QUIC	1292	Protected Payload (KP0)
990	5.815777	142.250.180.164	10.0.2.15	QUIC	1292	Protected Payload (KP0)
991	5.815777	142.250.180.164	10.0.2.15	QUIC	1292	Protected Payload (KP0)
992	5.815777	142.250.180.164	10.0.2.15	QUIC	1292	Protected Payload (KP0)
993	5.816274	142.250.180.164	10.0.2.15	QUIC	1292	Protected Payload (KP0)
994	5.816274	142.250.180.164	10.0.2.15	QUIC	1292	Protected Payload (KP0)
995	5.816274	142.250.180.164	10.0.2.15	QUIC	1007	Protected Payload (KP0)
996	5.838631	10.0.2.15	142.250.180.164	QUIC	78	Protected Payload (KP0), DCID=ebec5381582ad210

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface
> Ethernet II, Src: PCSSystemtec_e0:a8:ee (08:00:27:e0:a8:ee), Dst: 52:54:00
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 59013, Dst Port: 53
> Domain Name System (query)



Redeem a Steam Gift Card or W +

skeanmcoommumnity.com/formula/get/oere

STEAM® STORE COMMUNITY ABOUT SUPPORT

Your Store New & Noteworthy Categories Points Shop News Labs search

YOU RECEIVED A \$50 GIFT CARD TO YOUR BALANCE

CHOOSE AN OPTION TO GET STARTED

You must be logged into your Steam account to activate the gift card..

SIGN IN

Steam Gift Cards and Wallet Codes are an easy way to put money into your own Steam Wallet or give the perfect gift of games to your friend or family member.

Steam Gift Cards and Wallet Codes work just like gift certificates, which can be redeemed on Steam for the purchase of games, software, and any other item you can purchase on Steam. You can find Steam Gift Cards and Wallet Codes at retail stores across the world in a variety of denominations.

Note: Steam Gift Cards and Wallet Codes will be converted to the currency of your Steam Wallet upon redemption, regardless of where they were purchased.

Frequently asked questions about Wallet Codes



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.

The screenshot shows the VirusTotal analysis interface for the URL <https://skeanmcoommumnity.com/formula/get/oere>. The interface includes a summary card with a 'Community Score' of 3/96, a note that 3/96 security vendors flagged the URL as malicious, and details about the URL (Status 404, Content type application/json; charset=utf-8). Below this, a table lists vendor analysis results:

Vendor	Detection	Notes
Forcepoint ThreatSeeker	⚠️ Phishing	Malicious
Webscarab	⚠️ Malicious	Clean
Acronis	✓ Clean	Clean
AllLabs (MONITORAPP)	✓ Clean	Clean
alphaMountain.ai	✓ Clean	Clean
Netcraft		Malicious
Abusix		Clean
ADMINUSLabs		Clean
AlienVault		Clean
Antiy-AVL		Clean



```
Amministratore: Command Prompt + ▾
FLARE-VM 17/10/2024 17:22:05,77
C:\Users\flare\Desktop>ping is.gd

Esecuzione di Ping is.gd [172.67.83.132] con 32 byte di dati:
Risposta da 172.67.83.132: byte=32 durata=53ms TTL=50
Risposta da 172.67.83.132: byte=32 durata=52ms TTL=50

Statistiche Ping per 172.67.83.132:
  Pacchetti: Trasmessi = 2, Ricevuti = 2,
  Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
  Minimo = 52ms, Massimo = 53ms, Medio = 52ms
Control-C
^C
FLARE-VM 17/10/2024 17:22:26,09
C:\Users\flare\Desktop>ping skeanmcoommunnlty.com

Esecuzione di Ping skeanmcoommunnlty.com [104.21.16.39] con 32 byte di dati:
Risposta da 104.21.16.39: byte=32 durata=46ms TTL=52
Risposta da 104.21.16.39: byte=32 durata=45ms TTL=52

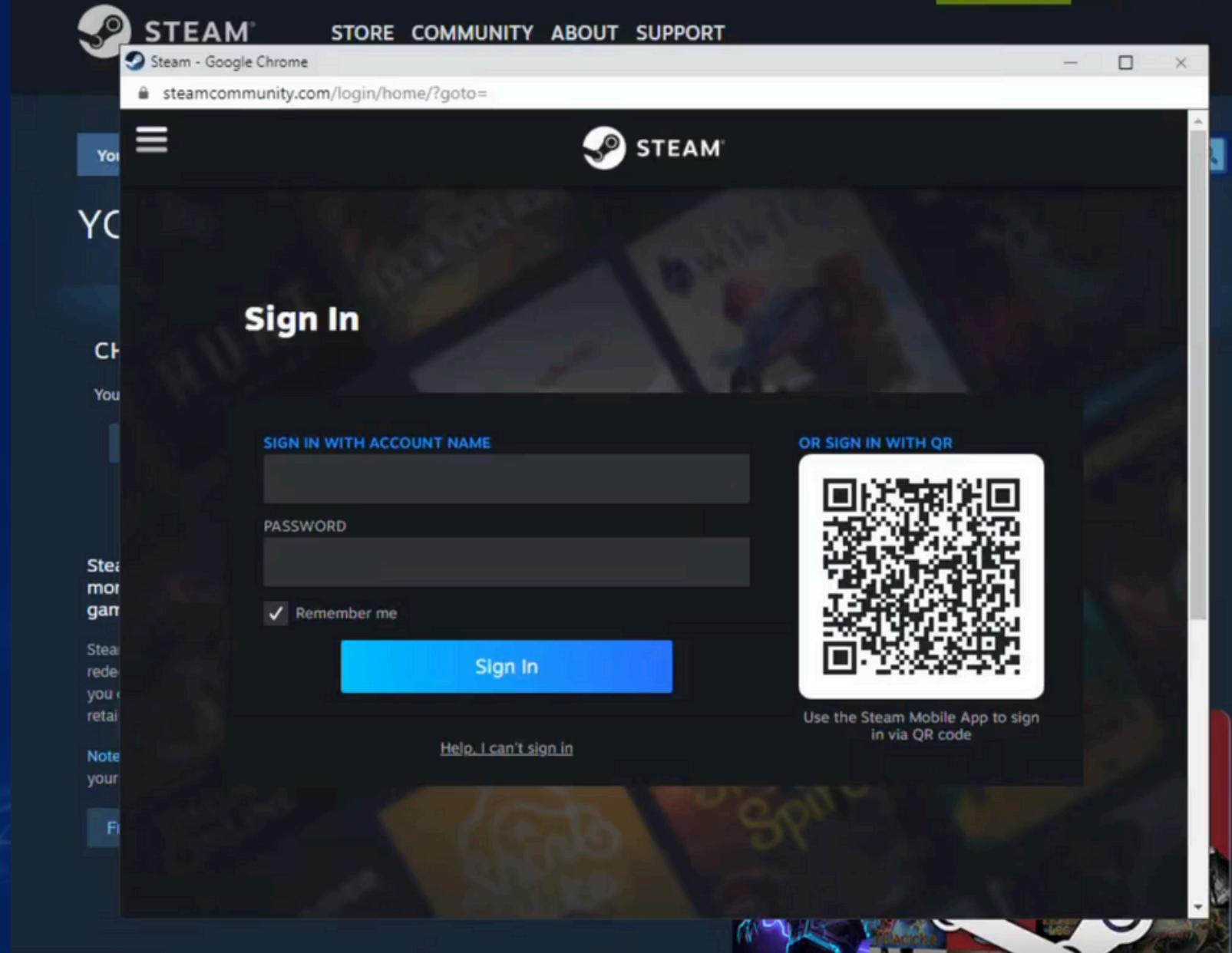
Statistiche Ping per 104.21.16.39:
  Pacchetti: Trasmessi = 2, Ricevuti = 2,
  Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
  Minimo = 45ms, Massimo = 46ms, Medio = 45ms
Control-C
^C
FLARE-VM 17/10/2024 17:23:34,90
C:\Users\flare\Desktop>
```

RINTRACCIAZIONE 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.

```
<!DOCTYPE html>
<html lang="en">
  <head> ...
  </head>
  <body>
    <noscript>You need to enable JavaScript to run this app.</noscript>
    <script>...
    <iframe id="main" title="site" name="site" style="outline: 0; border: none; position: absolute; top: 0; right: 0; left: 0; bottom: 0; width: 100vw !important; height: 100vh !important;">
      #document (<a href="https://skeanmcoommumnly.com/201f2d5_">https://skeanmcoommumnly.com/201f2d5_</a>)
        <!DOCTYPE html>
        <html class="responsive" lang="en">
          <head> ...
          <body class="v6 redeemwalletcode responsive_page">
            <div id="__ClassicStart"></div>
            ...
            <div class="responsive_page_frame with_header"> == $0
              <div class="responsive_page_menu_ctn mainmenu"> ...
                <div class="responsive_local_menu_tab"></div>
                <div class="responsive_page_menu_ctn localmenu"> ...
                  <div class="responsive_header"> ...
                    <div class="responsive_page_content_overlay"> </div>
                    <div class="responsive_fixonscroll_ctn nonresponsive_hidden"> ...
                </div>
            </div>
        </html>
      </div>
    </div>
  </body>
</html>
```

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.

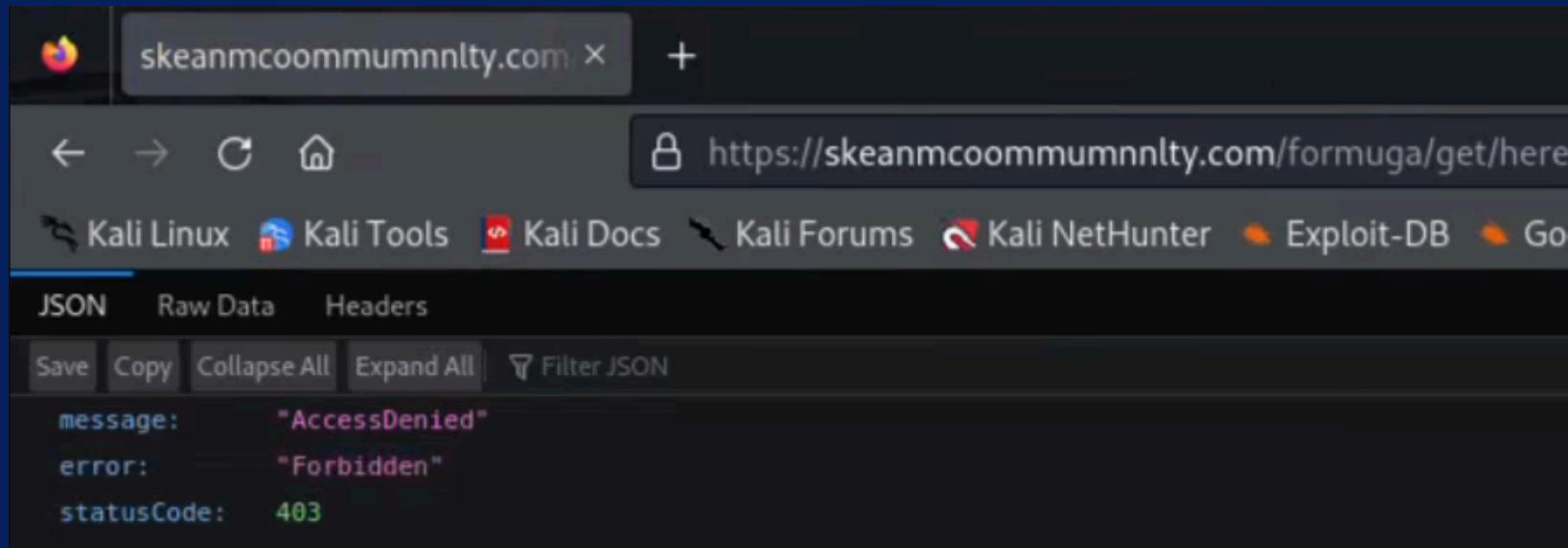


```
Keys added: 59
-----
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Mrt
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Mrt\_Merged
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Mrt\_Merged\Microsoft.Windows.SechHealthUI_cw5n1h2txyewy
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2408
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\W32:00000000000503E2
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-F11DB897C5CC7}
HKU\S-1-5-21-1839662007-3034634610-3909665979-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\4\Shell\{5C4F28B5-F869-4E84-8E60-F11DB897C5CC7}
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.

