BW3 es.2.2 Analisi Link

Informazioni Generali - General Information

⚜️ **Tag:** #analisi_generale #sicurezza #malware

- **Data di Analisi**: 25 agosto 2024, alle 22:44:49
- **Strumento di Analisi Utilizzato**: ANY.RUN - Malware Sandbox Online
- **Sistema Operativo Analizzato**: Windows 10 Professional (build 19045, 64 bit)

Descrizione dell'Analisi - Analysis Description

⚜️ **Tag:** #analisi_link #sandbox #anyrun

L'analisi è stata condotta sul link:

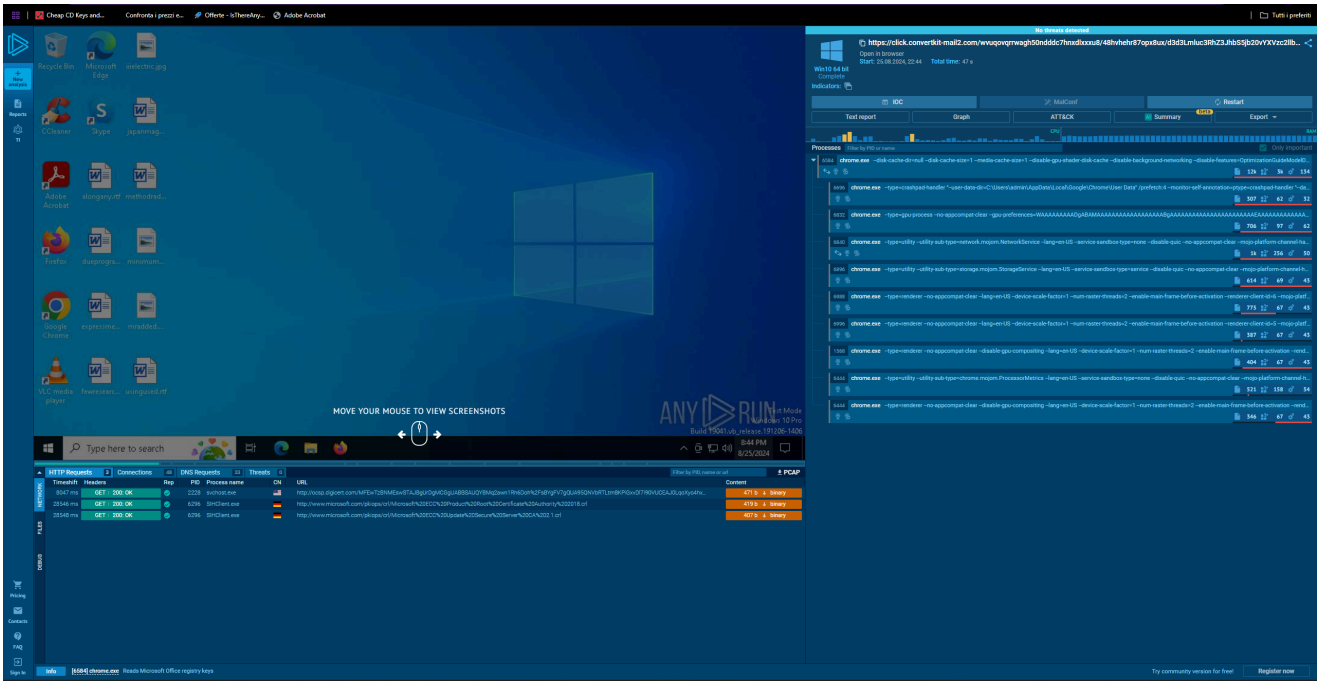
```
https://click.convertkit-mail2.com/wvuqovqrrwagh50ndddc7hnxdlxxxu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2llbnVyc2VyZWNydWl0ZXJz
```

Utilizzando la sandbox online **ANY.RUN**, l'analisi non ha identificato minacce malevole o indicatori sospetti associati al link. La sessione di monitoraggio ha avuto una durata complessiva di **300 secondi** durante i quali vari processi e attività di rete sono stati analizzati in dettaglio.

Risultati Principali - Main Findings

⚜️ **Tag:** #risultati #sicurezza #verodato

- **Verdetto**: Nessuna minaccia rilevata.
- **Indicatori di Malware**: Nessun indicatore malevolo o sospetto identificato.
- **Processi Analizzati**: 139 processi monitorati senza rilevazioni dannose.
- **Attività di Rete**:
  - **Richieste HTTP(S)**: 3
  - **Connessioni TCP/UDP**: 48
  - **Richieste DNS**: 33
  - Nessuna attività di rete è stata giudicata minacciosa.



Conclusione - Conclusion

⚜️ **Tag:** #conclusione #vero_negativo #sicurezza

L'analisi del link tramite la sandbox online **ANY.RUN** non ha rilevato alcuna minaccia malevola o indicatori sospetti. Tuttavia, è consigliato mantenere cautela nell'aprire link da fonti sconosciute, soprattutto in contesti pubblici.

Remediation - Remediation

⚜️ **Tag:** #remediation #protocollo_sicurezza #vero_negativo

Situazione di Vero Negativo: L'analisi ha identificato correttamente l'assenza di minacce, classificando il link come privo di rischi. Non sono necessarie azioni di mitigazione come la quarantena, l'eliminazione, l'inserimento in blacklist, o l'invio a un vendor per ulteriore analisi. Questo risultato è classificabile come **Vero Negativo** in quanto la mancanza di minacce è accurata e rispecchia la reale assenza di comportamenti sospetti o malevoli.

Motivazione: Un **vero negativo** si verifica quando una valutazione di sicurezza non rileva minacce reali, confermando l'affidabilità del sistema di rilevamento.

🔑 **Chiavi:**
[analisi link, vero negativo, sicurezza, malware, ANY.RUN, sandbox, attività di rete, remediation]

Approfondimento Link

⚜️ **Tag:** #analisi_malware #sandbox #processo

Questo report si concentra sull’analisi del link e dei processi avviati dal browser Google Chrome in un ambiente sandbox ANY.RUN, al fine di verificare eventuali minacce di esfiltrazione dati o comportamenti malevoli.

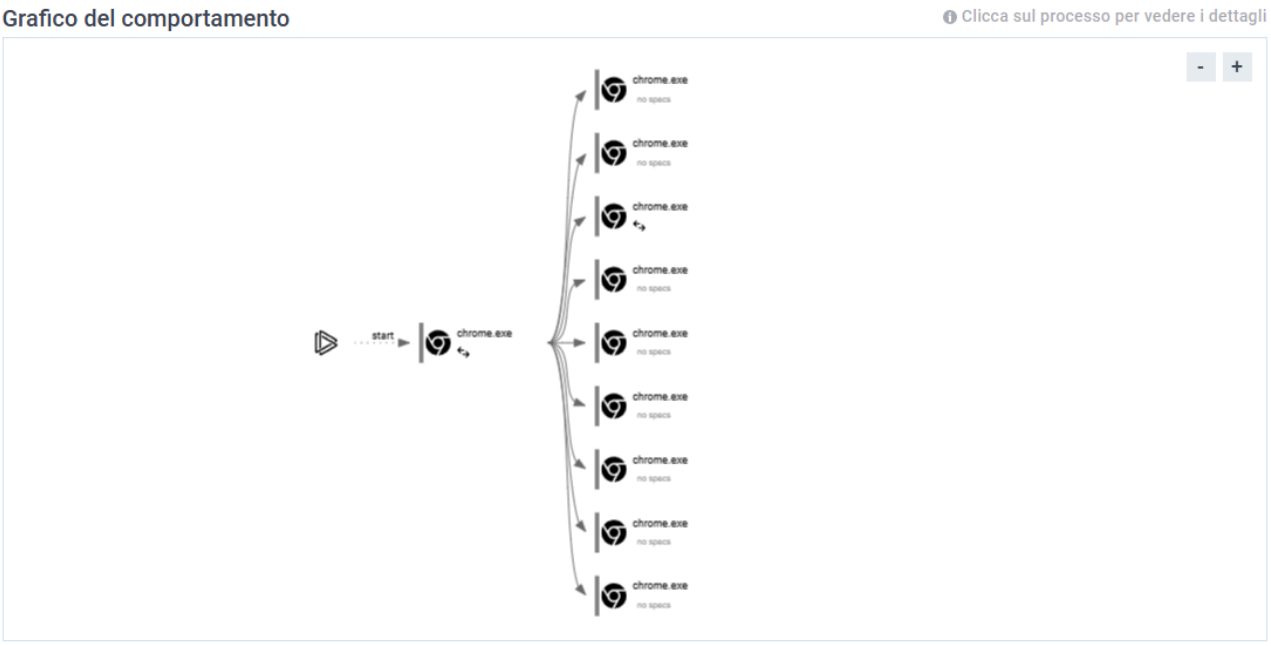
- **Link Analizzato**: https://click.convertkit-mail2.com/wvuqovqrrwagh50ndddc7hnxdlxxxu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2llbnVyc2VyZWNydWl0ZXJz
- **Ambiente**: Windows 10 Professional (build 19045, 64-bit)
- **Verdetto**: Nessuna minaccia rilevata【8†source】【14†source】.

Processi e Attività di Sistema - Processes and System Activity

⚜️ **Tag:** #processi #attivita_sistema #chrome

Processi Monitorati

1. **Totale dei Processi Avviati**: 139
2. **Processi Sospetti**: 0
3. **Processi Malevoli**: 0
4. **Processi Specifici di Chrome**:
   - Vari processi di Google Chrome sono stati avviati, includendo componenti come `renderer`, `gpu-process`, e `utility`.
   - **PID Principale**: 6584 - Chrome.exe【14†source】.



Attività del Registro di Sistema

- **Modifiche chiavi registro**: Interventi su chiavi legate a Chrome, come `HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\BLBeacon`.
- **Operazioni di Scrittura**: Numerose voci modificate, indicative di aggiornamenti interni del browser ma senza rilevare comportamenti anomali o malevoli.

Attività di File

- Chrome ha creato e aggiornato vari file temporanei e di log in directory specifiche, come:
  - `chrome_cart_db`, `coupon_db`, `sync_data`, con hash identificativi che non risultano malevoli (MD5 e SHA256 non associati a minacce note)【14†source】.

Sicurezza e Verifica di Esfiltrazione - Security and Exfiltration Checks

⚜️ **Tag:** #esfiltrazione #sicurezza #rete

Attività di Rete

1. **Richieste HTTP(S)**: 3
2. **Connessioni TCP/UDP**: 48
3. **Richieste DNS**: 33
4. **Analisi Esfiltrazione**: Nessun comportamento sospetto rilevato nelle comunicazioni di rete; tutte le richieste risultano su domini noti e affidabili (e.g., Google, Microsoft, Facebook) con connessioni HTTPS crittografate.

Indicatori di Minacce

- **Indicatori di Malware**: Nessun indicatore di malware o sospetto.
- **Esfiltrazione Dati**: Nessuna attività o processo ha suggerito tentativi di esfiltrazione o comunicazione verso IP o domini sconosciuti o sospetti.

Conclusione e Verdetto Finale - Conclusion and Final Verdict

⚜️ **Tag:** #conclusione #verdetto

L'analisi tramite ANY.RUN non ha riscontrato comportamenti sospetti o malevoli nei processi di Chrome né attività di rete associate a minacce. Il sistema risulta pulito e l'analisi si classifica come **Vero Negativo**, senza la necessità di interventi di mitigazione【14†source】.

🔑 **Chiavi:**
[anyrun, chrome, processo di analisi, esfiltrazione, sicurezza, registro di sistema, rete, vero negativo]

Per ulteriori informazioni consultare il report in allegato: ANY.RUN es.2.2.pdf

ANY RUN
INTERACTIVE MALWARE ANALYSIS

Informazioni generali

Indirizzo:	https://click.convertkit-mail2.com/wvuqovqrrwagh50ndddc7hnxdlxxxu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2llbnVyc2VyZWNydWl0ZXJz
Analisi completa:	https://app.any.run/tasks/f1f20828-2222-46fb-a886-09f77581e67b
Verdetto:	Nessuna minaccia rilevata
Data di analisi:	25 agosto 2024 alle 22:44:49
Sistema operativo:	Windows 10 Professional (build: 19045, 64 bit)
Indicatori:	
MD5:	4C091A5A8C03EBC2EA267980D0DA9F8D
SHA1:	F52CB78B7F23559FFCE5D1125EFD7B399165DFFC
Codice SHA256:	6DF8AB4ACFC5C751F09F2C8632464C8C5E6DA9D04539A69EDB0FC53CB561DFBC
SSDEEP:	3:N8UEGGy3I5lbdIJTQTT4SEfGSNscTNKdSVKBf0b/FIzfaLzw/y8aX:2UELmiTQTT4S8G+suGSgh0b/FIzAiaX

Set di ambiente software e opzioni di analisi

Configurazione di avvio

Durata dell'attività:	300 secondi	**Opzione Evasione Pesante:**	spento	**Geolocalizzazione della rete:**	spento
Tempo aggiuntivo utilizzato:	240 secondi	**Proxy MITM:**	spento	**Riservatezza:**	Presentazione pubblica
Opzione Fakenet:	spento	**Percorso tramite Tor:**	spento	**Autoconferma dell'UAC:**	SU
Rete:	SU				

Preimpostazione software

- Versione di Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64 bit) (23.001.20093)
- Versione 32.0.0.465 di Adobe Flash Player
- Versione PPAPI di Adobe Flash Player 32 (32.0.0.465)
- Pulizia di C (6.20)
- Versione 3.65.0 (3.65.0)
- Versione di Google Chrome (122.0.6261.70)
- Aiuto per gli aggiornamenti di Google (1.3.36.51)
- Aggiornamento Java 8 271 (64 bit) (8.0.2710.9)
- Aggiornamento automatico Java (2.8.271.9)
- Versione di Microsoft Edge (122.0.2365.59)
- Aggiornamento di Microsoft Edge (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - en-us (16.0.16026.20146)
- Microsoft Office Professional 2019 - es-es (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professionnel 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office профессиональный 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - en-us (16.0.16026.20146)
- Microsoft Update Health Tools (3.74.0.0)
- Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (123.0)
- Mozilla Maintenance Service (123.0)
- Notepad++ (64-bit x64) (7.9.1)
- Office 16 Click-to-Run Extensibility Component (16.0.15726.20202)
- Office 16 Click-to-Run Licensing Component (16.0.16026.20146)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202)
- Office 16 Click-to-Run Localization Component (16.0.15928.20198)
- PowerShell 7-x64 (7.3.5.0)
- Skype version 8.104 (8.104)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.59.0.0)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.63.0.0)

Hotfixes

- Client LanguagePack Package
- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face Package
- Hello Face Package
- InternetExplorer Optional Package
- InternetExplorer Optional Package
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- LanguageFeatures Basic en us Package
- LanguageFeatures Handwriting en us Package
- LanguageFeatures OCR en us Package
- LanguageFeatures Speech en us Package
- LanguageFeatures TextToSpeech en us Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MediaPlayer Package
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- OpenSSH Client Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- Printing PMCPPC FoD Package