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:N8UEGGy3I5lbdlJTQTT4SEfGSNscTNKdSVKBf0b/FlzfaLzw/y8aX:2UELmiTQTT4S8G+suGSgh0b/FlzAiaX

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

- Update for Windows 10 for x64-based Systems (KB4480730) (2.55.0.0)
- Update for Windows 10 for x64-based Systems (KB5001716) (8.93.0.0)
- VLC media player (3.0.11)
- WinRAR 5.91 (64-bit) (5.91.0)
- Windows PC Health Check (3.6.2204.08001)

- Printing PMCPPC FoD Package
- Printing PMCPPC FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- ProfessionalEdition
- ProfessionalEdition
- QuickAssist Package
- QuickAssist Package
- RollupFix
- RollupFix
- ServicingStack
- ServicingStack
- ServicingStack 3989
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- TabletPCMath Package
- TabletPCMath Package
- UserExperience Desktop Package
- UserExperience Desktop Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package

Attività comportamentali

MALIZIOSO

Nessun indicatore malevolo.

SOSPETTOSO

Nessun indicatore sospetto.

INFORMAZIONI

Legge le chiavi del registro di Microsoft Office

- chrome.exe (PID: 6584)

L'applicazione si è avviata da sola

- chrome.exe (PID: 6584)

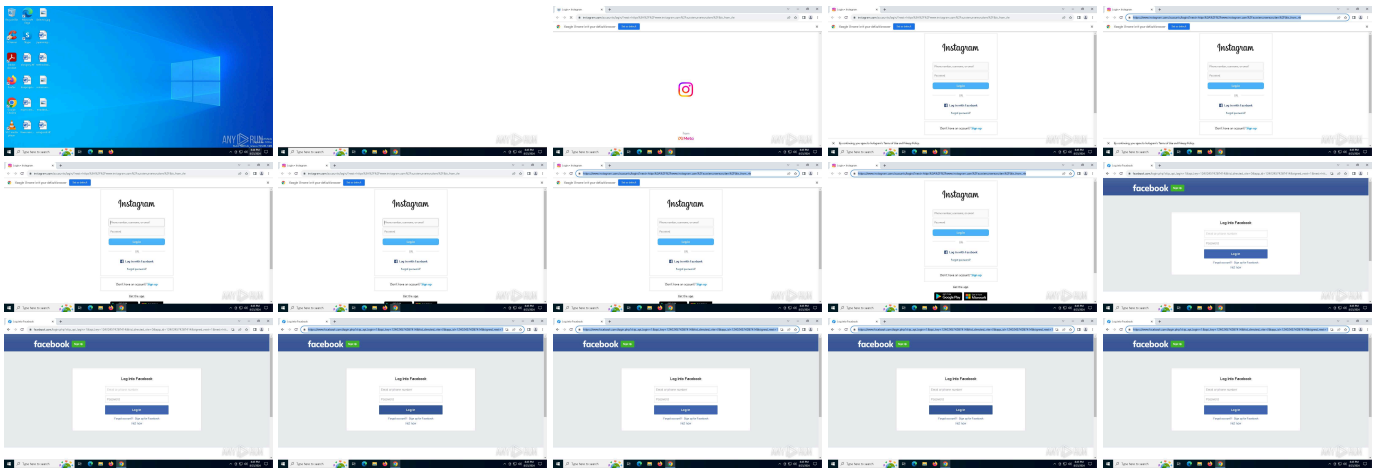
Configurazione del malware

Nessuna configurazione Malware.

Informazioni statiche

Nessun dato.

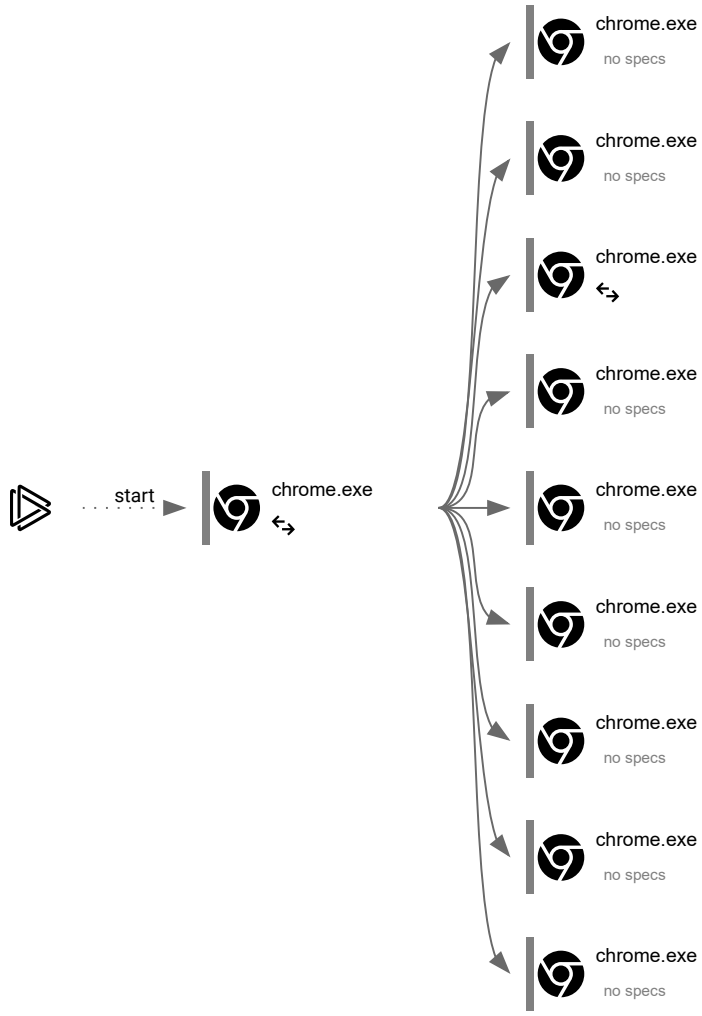
Video e screenshot



Processi

Processi totali	Processi monitorati	Processi dannosi	Processi sospetti
139	10	0	0

Grafico del comportamento



Descrizione delle specifiche

- Program did not start
- Probably Tor was used
- Known threat
- Connects to the network
- Task contains several apps running
- File is detected by antivirus software
- The process has the malware config
- Low-level access to the HDD
- Behavior similar to spam
- RAM overrun
- CPU overrun
- Application downloaded the executable file
- Inspected object has suspicious PE structure
- Process was added to the startup
- Task has injected processes
- Network attacks were detected
- Process starts the services
- Actions similar to stealing personal data
- Behavior similar to exploiting the vulnerability
- Debug information is available
- Executable file was dropped
- Integrity level elevation
- System was rebooted
- Task has apps ended with an error
- Task contains an error or was rebooted

Informazioni sul processo

PID	Comando	Sentiero	Indicatori	Processo padre
6584	"C:\Programmi\Google\Chrome\Application\chrome.exe" --disk-cache-dir=null --disk-cache-size=1 --media-cache-size=1 --disable-gpu-shader-disk-cache --disable-background-networking --disable-features=OptimizationGuideModelDownloading,OptimizationHintsFetching,OptimizationTargetPrediction,OptimizationHints "https://click.convertkit-mail2.com/wvuqovqrrwagh50ndddc7hnxdlxxxu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2llbnVyc2VyZWNydWl0ZXJz"	C:\Programmi\Google\Chrome\Application\chrome.exe		esploratore.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	MEDIO	**Descrizione:**	Google Chrome
Versione:	122.0.6261.70		

6696	"C:\Programmi\Google\Chrome\Application\chrome.exe" --type=crashpad-handler "--user-data-dir=C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Crashpad" --url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win64 --annotation=prod=Chrome --annotation=ver=122.0.6261.70 --dati-iniziali-client=0x224,0x228,0x22c,0x1f8,0x230,0x7fffd55cdc40,0x7fffd55cdc4c,0x7fffd55cdc58	C:\Programmi\Google\Chrome\Application\chrome.exe	—	cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	MEDIO	**Descrizione:**	Google Chrome
Versione:	122.0.6261.70		

6832	"C:\Programmi\Google\Chrome\Application\chrome.exe" --type=gpu-process --no-appcompat-clear --gpu-preferences=WAAAAAAAAAADgABAMAAAAAAAAAAAAAAAAAABgAAAAAAAA4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAAAYAAAAAAAAAAAAgAAAAAAAAACAAAAAAAAAAAAAAAAAAAAAAAA== --mojo-platform-channel-handle=1844 --field-trial-handle=1848,i,10703977562591596832,15426365956786484124,262144 --disable-features=Download del modello di guida all'ottimizzazione,Suggerimenti per l'ottimizzazione,Recupero di suggerimenti per l'ottimizzazione,Previsione del target di ottimizzazione --variations-seed-version /prefetch:2	C:\Programmi\Google\Chrome\Application\chrome.exe	—	cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	BASSO	**Descrizione:**	Google Chrome
Versione:	122.0.6261.70		

6840	"C:\Programmi\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --disable-quic --no-appcompat-clear --mojo-platform-channel-handle=2092 --field-trial-handle=1848,i,10703977562591596832,15426365956786484124,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:3	C:\Programmi\Google\Chrome\Application\chrome.exe	⇆	cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	MEDIO	**Descrizione:**	Google Chrome
Versione:	122.0.6261.70		

6896	"C:\Programmi\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --disable-quic --no-appcompat-clear --mojo-platform-channel-handle=2060 --field-trial-handle=1848,i,10703977562591596832,15426365956786484124,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:8	C:\Programmi\Google\Chrome\Application\chrome.exe	—	cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	BASSO	**Descrizione:**	Google Chrome
Versione:	122.0.6261.70		

6988	"C:\Programmi\Google\Chrome\Application\chrome.exe" --type=renderer --no-appcompat-clear --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=6 --mojo-platform-channel-handle=3052 --field-trial-handle=1848,i,10703977562591596832,15426365956786484124,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:1	C:\Programmi\Google\Chrome\Application\chrome.exe	—	cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	BASSO	**Descrizione:**	Google Chrome
Codice di uscita:	0	**Versione:**	122.0.6261.70

6996	"C:\Programmi\Google\Chrome\Application\chrome.exe" --type=renderer --no-appcompat-clear --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=5 --mojo-platform-channel-handle=3068 --field-trial-handle=1848,i,10703977562591596832,15426365956786484124,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:1	C:\Programmi\Google\Chrome\Application\chrome.exe	—	cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	BASSO	**Descrizione:**	Google Chrome
Codice di uscita:	0	**Versione:**	122.0.6261.70

1568	"C:\Programmi\Google\Chrome\Application\chrome.exe" --type=renderer --no-appcompat-clear --disable-gpu-compositing --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=7 --mojo-platform-channel-handle=4036 --field-trial-handle=1848,i,1070397756259159683 2,15426365956786484124,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /precarica:1	C:\Programmi\Google\Chrome\Application\chrome.exe	–	cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	BASSO	**Descrizione:**	Google Chrome
Versione:	122.0.6261.70		

6444	"C:\Programmi\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.ProcessorMetrics --lang=en-US --service-sandbox-type=none --disable-quic --no-appcompat-clear --mojo-platform-channel-handle=4716 --field-trial-handle=1848,i,1070397756259159683 2,15426365956786484124,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:8	C:\Programmi\Google\Chrome\Application\chrome.exe	–	cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	MEDIO	**Descrizione:**	Google Chrome
Codice di uscita:	0	**Versione:**	122.0.6261.70

6444	"C:\Programmi\Google\Chrome\Application\chrome.exe" --type=renderer --no-appcompat-clear --disable-gpu-compositing --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=9 --mojo-platform-channel-handle=4728 --field-trial-handle=1848,i,1070397756259159683 2,15426365956786484124,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /precarica:1	C:\Programmi\Google\Chrome\Application\chrome.exe	–	cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	BASSO	**Descrizione:**	Google Chrome
Versione:	122.0.6261.70		

Attività del registro

Eventi totali	Leggi gli eventi	Scrivi eventi	Elimina eventi
4 567	4 549	18	0

Eventi di modifica

(PID) Processo:	(6584) chrome.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\BLBeacon
Operazione:	scrivere	**Nome:**	conteggio_falliti
Valore:	0		

(PID) Processo:	(6584) chrome.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\BLBeacon
Operazione:	scrivere	**Nome:**	stato
Valore:	2		

(PID) Processo:	(6584) chrome.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\Terze parti
Operazione:	scrivere	**Nome:**	Codici di stato
Valore:			

(PID) Processo:	(6584) chrome.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\Terze parti
Operazione:	scrivere	**Nome:**	Codici di stato
Valore:	01000000		

(PID) Processo:	(6584) chrome.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\BLBeacon
Operazione:	scrivere	**Nome:**	stato

Valore: 1

(PID) Processo: (6584) chrome.exe **Chiave:** HKEY_CURRENT_USER\SOFTWARE\Google\Aggiorna\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operazione: scrivere **Nome:** dottore
Valore: 1

(PID) Processo: (6584) chrome.exe **Chiave:** HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\StabilityMetrics
Operazione: scrivere **Nome:** metriche_dell'esperienza_utente.stabilità.uscito_pulito
Valore: 0

(PID) Processo: (6584) chrome.exe **Chiave:** HKEY_CURRENT_USER\SOFTWARE\Google\Chrome
Operazione: scrivere **Nome:** Statistiche di utilizzo nel campione
Valore: 0

(PID) Processo: (6584) chrome.exe **Chiave:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Google\Update\ClientStateMedium\{8A69D345-D564-463C-AFF1-A69D9E530F96}
Operazione: scrivere **Nome:** statistiche di utilizzo
Valore: 0

(PID) Processo: (6584) chrome.exe **Chiave:** HKEY_CURRENT_USER\SOFTWARE\Google\Aggiorna\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operazione: scrivere **Nome:** metricaid
Valore:

(PID) Process: (6584) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** metricsid_installdate
Value: 0

(PID) Process: (6584) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** metricsid_enableddate
Value: 0

(PID) Process: (6584) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** lastrun
Value: 13369092300062148

Attività dei file

File eseguibili	File sospetti	File di testo	Tipi sconosciuti
0	30	18	2

File eliminati

PID	Processo	Nome file	Tipo
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\chrome_cart_db\LOG.old **MD5:** — **Codice SHA256:** —	—
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\parcel_tracking_db\LOG.old **MD5:** — **Codice SHA256:** —	—
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\PersistentOriginTrials\LOG.old **MD5:** — **Codice SHA256:** —	—
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\coupon_db\LOG.old~RF11ef4f.TMP **MD5:** — **Codice SHA256:** —	—
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\coupon_db\LOG.old **MD5:** — **Codice SHA256:** —	—
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\discounts_db\LOG.old **MD5:** — **Codice SHA256:** —	—
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\commerce_subscription_db\LOG.old~RF11ef5e.TMP **MD5:** — **Codice SHA256:** —	—
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\commerce_subscription_db\LOG.old **MD5:** — **Codice SHA256:** —	—
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\Archiviazione locale\leveldb\LOG.old~RF11f039.TMP **MD5:** 390E3C6EDCE7036BB6F52670DC24ABAD **Codice SHA256:** D6F1B47CD05A8E1FAD989DEEC22ED67EA9A013C2DE0CCAFD68A539F69BD0DD70	testo
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Ultima versione **MD5:** FCE53E052E5CF7C20819320F374DEA88 **Codice SHA256:** CD95DE277E746E92CC2C53D9FC92A8F6F0C3EDFB7F1AD9A4E9259F927065BC89	testo
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old **MD5:** 19D1A06251A8678F85D8DE5BFAB83807 **SHA256:** AA6E55DCF84CDAF0BD3F913E7B837F65500E9B71A5A7AA773D02FFBC18C7FF01	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old	text

		MD5: 723783C35EAEEE1492EDB30847AE6750 **SHA256:** C29323F784CF873BF34992E7A2B4630B19641BF42980109E31D5AF2D487DF6F8	
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old **MD5:** F96D0EF8D63094D714514A441F8CD3FB **SHA256:** 2083625CA1E32D366F0B664D9B87B591791EF2EA2B770F4FA6ABE13FECA01196	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old **MD5:** A95974F48FC4A0E16E9D7729D7874157 **SHA256:** 926422473F59B7759EA8EB2064FD6DF9D00A88B548DEF1D5C3E08860357C03A2	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old~RF11f0a6.TMP **MD5:** 13D19AD173F46FFCD5871A3309D723EF **SHA256:** F74346A518C9CA378DE81E9459ACB62FE0B1B6CE4CD9F190D0729A40B75B46F3	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old~RF1208e1.TMP **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old~RF1208e1.TMP **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SignalDB\LOG.old~RF1208e1.TMP **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SignalDB\LOG.old **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old~RF1208e1.TMP **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\aacde8be-d8b2-42a7-86e3-ee75d830105d.tmp **MD5:** 5058F1AF8388633F609CADB75A75DC9D **SHA256:** CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old **MD5:** 668BAE5C0A00EF466FA52102A122346C **SHA256:** A366BA8B2FD21BB25B17C6AC8A2C07428AEE94E6EA8CB14E204E4F77F61E2D40	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\LOG.old **MD5:** 4B26172585D38A3DD6697E274D0608AC **SHA256:** 85899A7AF1BD1939EA8264009EC427930FC5C092C8C3193984D6391526319268	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old~RF11ef2f.TMP **MD5:** 8F45965291AB2DA10EEB049FB6E917C6 **SHA256:** 8A0DE526945B27CDBBD87357C85FDDD37B572370F894CB0A5AC533FD465D2166	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old~RF11ef3f.TMP **MD5:** 139F545948FC1F10256A27E3C2CEF062 **SHA256:** 9399CC6F9C335015E086DB37208B1816A7831221A005B04AC83C4F86CC04230D	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old~RF12097e.TMP **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old~RF12098d.TMP **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old~RF12098d.TMP **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\a373af73-612c-4659-93d0-410a1718a8f0.tmp **MD5:** 3433CCF3E03FC35B634CD0627833B0AD **SHA256:** F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D	flc
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Variations **MD5:** 961E3604F228B0D10541EBF921500C86 **SHA256:** F7B24F2EB3D5EB0550527490395D2F61C3D2FE74BB9CB345197DAD81B58B5FED	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\LOG.old~RF11f0b6.TMP **MD5:** 4320BE33704F77FF4DF4921358D2C50C **SHA256:** 8FDF7387C47EB272670EFF935D71492F03EAFAA55A8B22C05658BB0F1AC472EE	text
6840	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\Trust Tokens **MD5:** 767A7DB34589653629C0D4299AA9EB7A **SHA256:** 78A4734F08B47286A3736C88C6FC481F76BD2B1A46E29D0920939F088CE899FD	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old **MD5:** DF81465C6FD3C271021EFEF60DC3C105 **SHA256:** C3099E8B290EC2DB598E8516BE5D963729363E0FB6D8C3F89131F9B747CDDA7F	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat **MD5:** FC81892AC822DCBB09441D3B58B47125 **SHA256:** FB077C966296D02D50CCBF7F761D2A3311A206A784A7496F331C2B0D6AD205C8	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old~RF11f0b6.TMP **MD5:** 602C51DB8380F8CD0A961D9A46AF1186 **SHA256:** 84F716E38017F52138A76222524A3152DB8D3A7FBE30E94067458568B14DC36D	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old~RF11f0d5.TMP	text

		MD5: 86E6BAA91A6F56387D777804EC3DE437 **SHA256:** BB32752B143D45A6914D496141D263991B7AA04ADD153D8BD8C736DE282A2A1A	
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\74c3a269-7813-4bd3-b470-f30a7ba1eab5.tmp **MD5:** BB775DDBB6D07D860A65C0EDF82FD1CF **SHA256:** C1634DCE95A867FFB2742F631884B03FFF8B21758129954DD6C29D7DAAB5A39E	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State~RF121601.TMP **MD5:** 6EF6D4132727E4F700645C341C4BEEE2 **SHA256:** 5164FDFC5C55D1BE643CF646E2E89C32191344D969632C8AED72922AE31D06C2	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\trusted_vault.pb **MD5:** 3433CCF3E03FC35B634CD0627833B0AD **SHA256:** F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D	flc
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\4fe5dd14-d7e3-41b6-af87-42d2c1bfdb82.tmp **MD5:** A6AD232FED1D99F06AAC9A509ED18705 **SHA256:** F3B581BC559838F9097C310B5697CF468A2827681BFD65F8C1BDD4FA42B4ABC6	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\271e80f4-bc28-486c-80b7-275e82a1abd1.tmp **MD5:** 83AA2B8DE0A9431B3D952EC13A935878 **SHA256:** 74BC9D136C079CC751B6D7CA2EC5155758D0834E9CE141541F6D485A6642058E	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF123dad.TMP **MD5:** BB775DDBB6D07D860A65C0EDF82FD1CF **SHA256:** C1634DCE95A867FFB2742F631884B03FFF8B21758129954DD6C29D7DAAB5A39E	binary
6840	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\a891b62e-0585-4a6b-84ad-cdd13adeb018.tmp **MD5:** 984AF758ACB0AF16EF5D6925096FD5D4 **SHA256:** DAF3050630467A5A74E3AB63D7FE954CAC3EE0797F155787A58E234649F0FF76	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF121630.TMP **MD5:** E4129B94C2087C5DC93A5CBEBAE43E4E **SHA256:** 5EFFB0299F4E0EA6DAD1B30234ECF8140810CEB74C40E11457A1CBAE8E93F0AA	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Last Browser **MD5:** DE9EF0C5BCC012A3A1131988DEE272D8 **SHA256:** 3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old~RF12097e.TMP **MD5:** 2BB5E5996BF5B9092AFEF1DB178D92D2 **SHA256:** 4F42BBC1849F98F282D3B12B63D6C7DFDCD037101229496BE326ABEEC1845302	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old **MD5:** 87F4E464F4EE3D5C7DA6FA24D1F52629 **SHA256:** F12400B717EF912F6A80A009E3CE2723854F8B057F066C2DD6FDF370657FBE55	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\trusted_vault.pb~RF11f20e.TMP **MD5:** 3433CCF3E03FC35B634CD0627833B0AD **SHA256:** F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D	flc
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF128c5a.TMP **MD5:** A6AD232FED1D99F06AAC9A509ED18705 **SHA256:** F3B581BC559838F9097C310B5697CF468A2827681BFD65F8C1BDD4FA42B4ABC6	binary
6840	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\59e7fb00-bf11-4056-8d03-c89a492e2bed.tmp **MD5:** B23767D97D2353AEA997CED612562380 **SHA256:** 76E4141C621912C8A999097AB35365E6CBE339A6E873204597172FF6C67FC620	binary
6988	chrome.exe	C:\Users\admin\AppData\Local\Temp\cfcb9fcb-e34f-4f50-9d44-27f054d6d7b4.tmp **MD5:** F5337ED0CDC217FE98ADB7A14FABD1AE **SHA256:** 3A63B8AF3FC416B1A5B204CA2AD9C067C10CD4E8C5D32043AD0D4C5EB95ACDDD	image
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State **MD5:** 83AA2B8DE0A9431B3D952EC13A935878 **SHA256:** 74BC9D136C079CC751B6D7CA2EC5155758D0834E9CE141541F6D485A6642058E	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences **MD5:** BB775DDBB6D07D860A65C0EDF82FD1CF **SHA256:** C1634DCE95A867FFB2742F631884B03FFF8B21758129954DD6C29D7DAAB5A39E	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\418b0f8a-b1e7-4053-bab5-b4715dae285a.tmp **MD5:** A9A97F75C1E9464A6DD580E8F13F8804 **SHA256:** B1EBED604DDC48C5E36FBE67B8CF78F1119B3979767BE26DAEE930BAB7079CC3	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF1264fc.TMP **MD5:** A9A97F75C1E9464A6DD580E8F13F8804 **SHA256:** B1EBED604DDC48C5E36FBE67B8CF78F1119B3979767BE26DAEE930BAB7079CC3	binary
6840	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\TransportSecurity **MD5:** B23767D97D2353AEA997CED612562380 **SHA256:** 76E4141C621912C8A999097AB35365E6CBE339A6E873204597172FF6C67FC620	binary
6840	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\TransportSecurity~RF1259ef.TMP **MD5:** B23767D97D2353AEA997CED612562380 **SHA256:** 76E4141C621912C8A999097AB35365E6CBE339A6E873204597172FF6C67FC620	binary
6840	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\de557ecd-aff3-4a37-9415-7a9e1a2b32b9.tmp **MD5:** B399D11176C4739232C037B987DAB8D7 **SHA256:** 04F01723E3F24EDB8737B954593527185DB2827C2F8F270C8F500A8FA122664A	binary
6840	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\TransportSecurity~RF12191e.TMP **MD5:** 501106C8FFCBFE805C6EF3727B140B3F **SHA256:** F63D1CF4F3F3287B792F20CA269EC790C7CCCB99DB9E083E633194716FC36E58	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\495dbd56-0fb8-4876-9e3c-2c42d0688a5d.tmp **MD5:** C0F2E46CF04EAF572389C66CDB6CEAB7 **SHA256:** 909333A028196840A8E9085D345110D063025045BF52BB191649B168576FC873	binary
6840	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\TransportSecurity~RF128313.TMP **MD5:** 984AF758ACB0AF16EF5D6925096FD5D4 **SHA256:** DAF3050630467A5A74E3AB63D7FE954CAC3EE0797F155787A58E234649F0FF76	binary

Attività di rete

Richieste HTTP(S)	Connessioni TCP/UDP	Richieste DNS	Minacce
3	48	33	0

Richieste HTTP

PID	Processo	Metodo	Codice HTTP	Proprietà intellettuale	Indirizzo URL	CN	Tipo	Misurare	Reputazione
6296	SIHClient.exe	OTTENERE	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	sconosciuto	–	–	sconosciuto
6296	SIHClient.exe	OTTENERE	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	sconosciuto	–	–	sconosciuto
2228	svchost.exe	OTTENERE	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	sconosciuto	–	–	sconosciuto

Connessioni

PID	Processo	Proprietà intellettuale	Dominio	ASN	CN	Reputazione
4	Sistema	192.168.100.255:138	–	–	–	inserito nella lista bianca
4436	svchost.exe	51.104.136.2:443	impostazioni-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCCO	CIOÈ	inserito nella lista bianca
608	RUXIMICS.exe	51.104.136.2:443	impostazioni-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCCO	CIOÈ	inserito nella lista bianca
2120	MoUsoCoreWorker.exe	51.104.136.2:443	impostazioni-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCCO	CIOÈ	inserito nella lista bianca
6584	cromo.exe	239.255.255.250:1900	–	–	–	inserito nella lista bianca
6840	cromo.exe	3.141.222.179:443	clicca.convertkit-mail2.com	AMAZZONIA-02	NOI	sconosciuto
6840	cromo.exe	66.102.1.84:443	account.google.com	GOOGLE	NOI	sconosciuto
6840	cromo.exe	157.240.0.174:443	www.instagram.com	FACEBOOK	NOI	sconosciuto
6840	cromo.exe	157.240.0.63:443	static.cdninstagram.com	FACEBOOK	NOI	sconosciuto
2228	svchost.exe	40.126.32.133:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCCO	NL	sconosciuto
3260	svchost.exe	40.113.110.67:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
2228	svchost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
6840	chrome.exe	157.240.0.35:443	www.facebook.com	FACEBOOK	US	unknown
6840	chrome.exe	142.250.186.138:443	content-autofill.googleapis.com	GOOGLE	US	whitelisted
6840	chrome.exe	172.217.16.196:443	www.google.com	GOOGLE	US	whitelisted
6584	chrome.exe	224.0.0.251:5353	–	–	–	unknown
6296	SIHClient.exe	20.12.23.50:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
6296	SIHClient.exe	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
6296	SIHClient.exe	52.165.164.15:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
6840	chrome.exe	157.240.0.6:443	static.xx.fbcdn.net	FACEBOOK	US	unknown
3888	svchost.exe	239.255.255.250:1900	–	–	–	whitelisted

Richieste DNS

Dominio	Proprietà intellettuale	Reputazione
impostazioni-win.data.microsoft.com	51.104.136.2	inserito nella lista bianca
google.com	172.217.16.206	inserito nella lista bianca
clicca.convertkit-mail2.com	3.141.222.179 3.18.56.123 18.220.225.51	sconosciuto
account.google.com	66.102.1.84	inserito nella lista bianca
www.instagram.com	157.240.0.174	inserito nella lista bianca

static.cdninstagram.com	157.240.0.63	sconosciuto
login.live.com	40.126.32.133 20.190.160.20 40.126.32.140 40.126.32.68 20.190.160.17 20.190.160.22 40.126.32.134 40.126.32.76	inserito nella lista bianca
client.wns.windows.com	40.113.110.67	inserito nella lista bianca
ocsp.digicert.com	192.229.221.95	inserito nella lista bianca
www.facebook.com	157.240.0.35	inserito nella lista bianca
content-autofill.googleapis.com	142.250.186.138 142.250.185.138 142.250.186.170 142.250.184.234 142.250.185.170 142.250.185.202 142.250.185.234 142.250.181.234 142.250.186.74 216.58.212.170 216.58.206.74 142.250.186.42 172.217.18.10 142.250.186.106 172.217.16.202 216.58.206.42	whitelisted
www.google.com	172.217.16.196	whitelisted
slscr.update.microsoft.com	20.12.23.50	whitelisted
www.microsoft.com	23.35.229.160	whitelisted
fe3cr.delivery.mp.microsoft.com	52.165.164.15	whitelisted
static.xx.fbcdn.net	157.240.0.6	whitelisted
facebook.com	157.240.0.35	whitelisted

Minacce

Nessuna minaccia rilevata

Stringhe di output di debug

Nessuna informazione di debug