Build Week 3 - ES 5 PARTE 2
Report di Analisi Sicurezza: Campagna Phishing "ConvertKit-Meta"

Data: 24/02/2026

Oggetto: Task 5 - Analisi di un ipotetico Agent Tesla

Target: Analisi Statica e Dinamica

1. Executive Summary

L'analisi del sample fornito, inizialmente sospettato di essere il malware "Agent Tesla", ha rivelato una minaccia di natura profondamente diversa. L'architettura mostrata dalle analisi condotte non ha a che fare con un file eseguibile o di un malware progettato per infettare fisicamente i computer aziendali.

Ci troviamo di fronte a una **campagna avanzata di Phishing e Credential Harvesting** (furto di credenziali). L'attaccante ha architettato una truffa basata su interfaccia web che abusa di servizi legittimi di invio email per aggirare i filtri di sicurezza e sfrutta l'infrastruttura reale di Meta (Facebook/Instagram) per ingannare l'utente. L'analisi del codice ha inoltre rivelato che la pagina è strutturata non solo per rubare password, ma anche per sottrarre documenti aziendali riservati.

1.1 Ipotesi della Minaccia (Classificazione)

- **Falso Positivo per "Agent Tesla":** Nessun eseguibile, keylogger o infostealer è stato scaricato sul sistema locale. L'endpoint è pulito.
- **Vero Positivo per "Advanced Credential Harvesting & OAuth Abuse":** L'attacco mira a sottrarre le credenziali e potenzialmente in grado di rubare sessioni (OAuth) manipolando i parametri URL di login legittimi.

---

2. Vettore di Infezione

La catena di compromissione si sviluppa in modo da eludere i controlli perimetrali aziendali:

1. **Phishing via Email:** L'utente riceve un'email contenente un link apparentemente innocuo.

2. **Bypass dei Filtri (SEG Evasion):** Il link non punta a un server malevolo, ma a `click.convertkit-mail2.com`.

   ConvertKit è una piattaforma legittima di email marketing; abusandone, l'attaccante garantisce che l'email superi i controlli antispam grazie all'alta reputazione del dominio.

3. **Reindirizzamento Dinamico:** Una volta cliccato il link, il server di ConvertKit traccia l'utente (registrando IP, User-Agent e orario) e lo reindirizza (tramite un codice HTTP 302) verso la trappola finale.

3. Analisi Tecnica Dettagliata (Technical Deep-Dive)

La valutazione dell'ambiente di esecuzione ha evidenziato l'assoluta pulizia a livello di rete e sistema operativo, spostando il focus sul livello applicativo.

3.1 Network & DNS Analysis

L'ispezione dei protocolli di trasporto (TCP/UDP) non ha rivelato comunicazioni verso server di Comando e Controllo (C2). Sono stati analizzati 4 pacchetti per scongiurare ogni possibile traffico malevolo mascherato da legittimo

Il traffico rilevato è stato classificato come "rumore fisiologico" di sistema:

- Traffico NetBIOS di Windows (UDP 138).

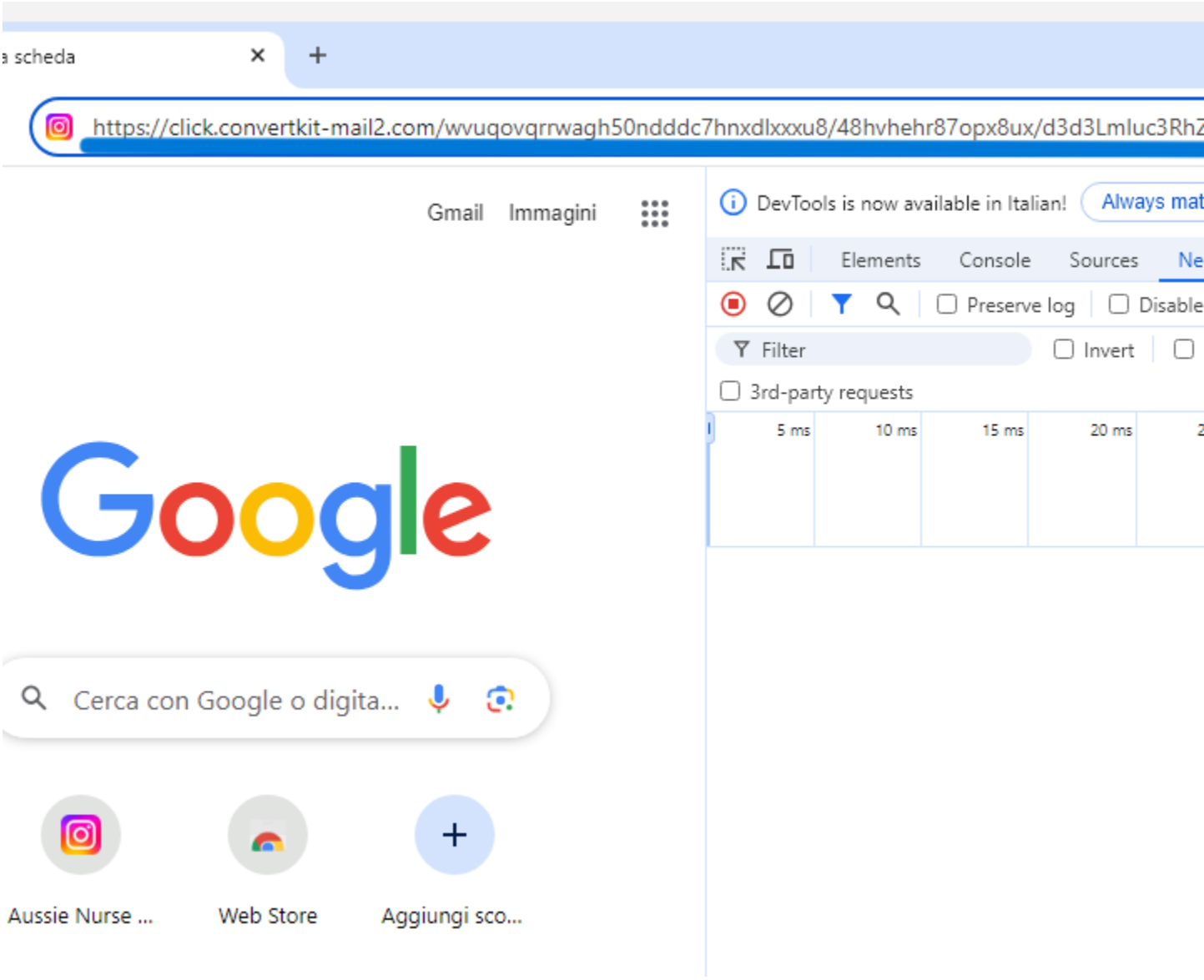
- Traffico SSDP e mDNS generato dal browser Chrome (UDP 1900, 5353) per la ricerca di dispositivi locali.

L'analisi DNS conferma l'assenza di server clone: il browser risolve direttamente i domini ufficiali di Meta (`www.instagram.com`, `static.cdninstagram.com`, `www.facebook.com`). L'utente visualizza **la vera pagina di login** , ma l'URL è stato manipolato (es. tramite i parametri `api_key` e `skip_api_login`) per dirottare l'autorizzazione dell'account verso un'app controllata dall'attaccante.

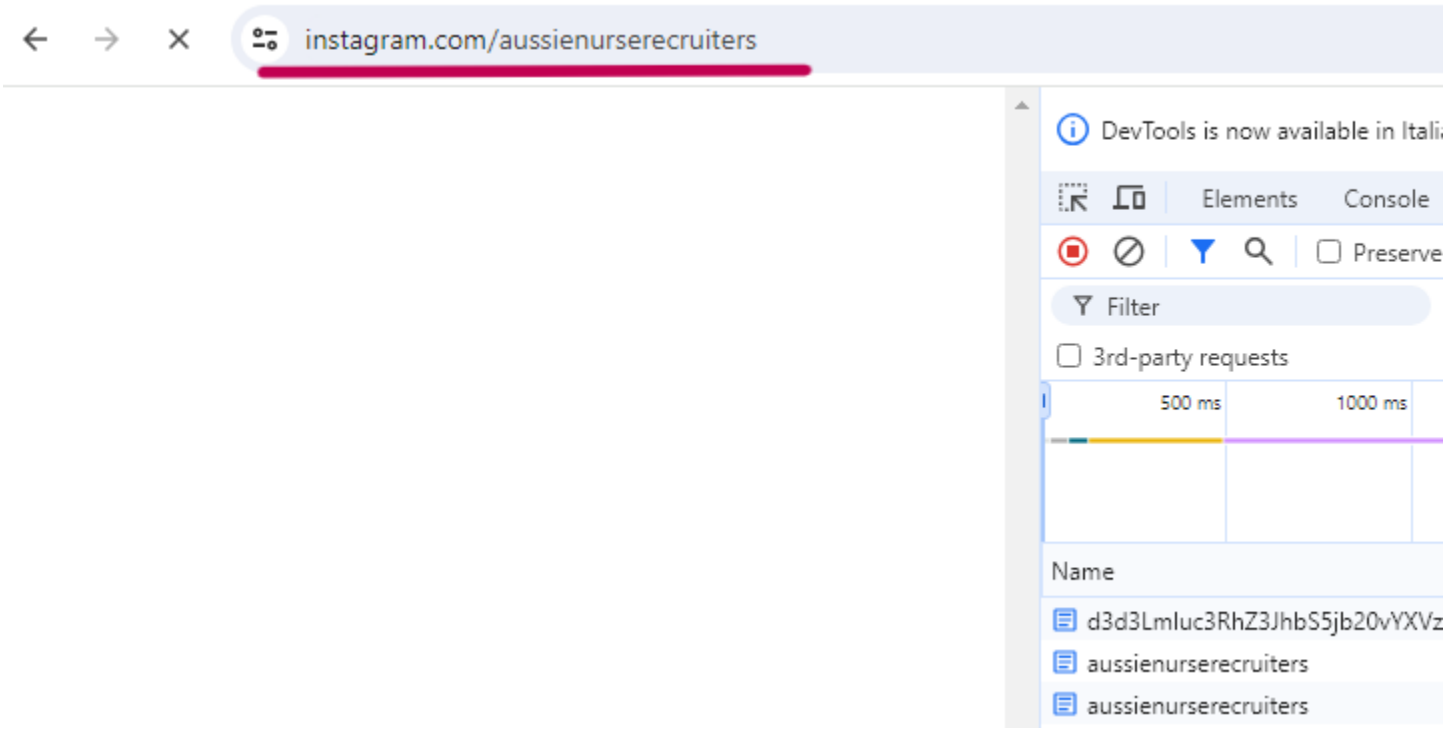
3.2 Analisi Applicativa (HTTP & Payload)

L'URL iniziale contiene un parametro codificato in Base64: `d3d3Lmluc3RhZ3JhbS5jb20vYXVzc21lbnVyc2VyZWNydWl0ZXJz`. Decodificandolo, si ottiene la reale destinazione del reindirizzamento: `www.instagram.com/aussienurserecruiters`. L'uso del Base64 permette all'attaccante di cambiare dinamicamente il bersaglio sfuggendo ai filtri statici.

Viene condotta un’analisi dinamica inserendo direttamente l’URL infetto nel proprio browser per capirne appieno il comportamento, di seguito viene illustrata la dinamica attraverso screenshot:

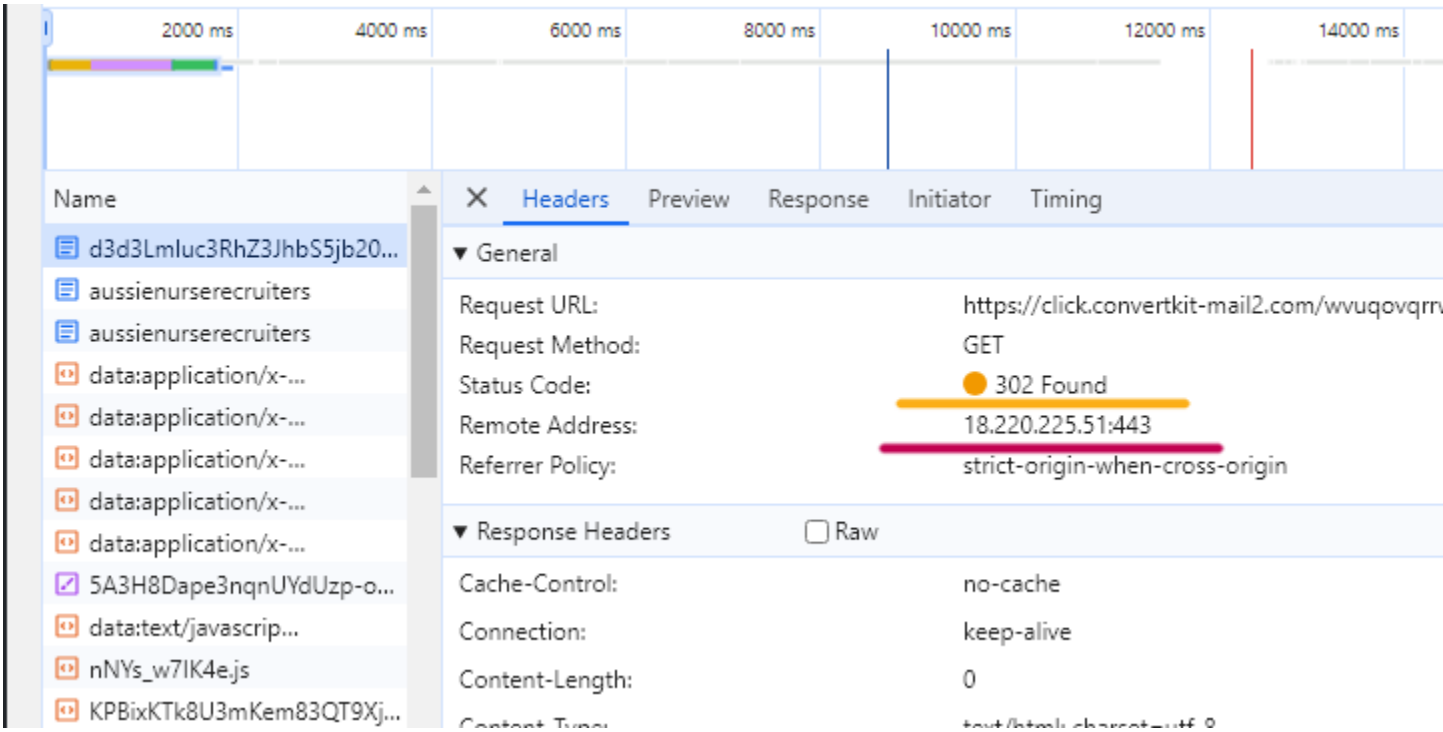


dopodiché viene avviato il reindirizzamento:



Il DNS risolve quelle stringhe di URL in base 64 viene risolto riportando alla pagina “Aussie Nurse Recruiters”

Nella sezione Network vengono mostrati metodi, indirizzo remoto e porta a cui saranno redirette le informazioni:

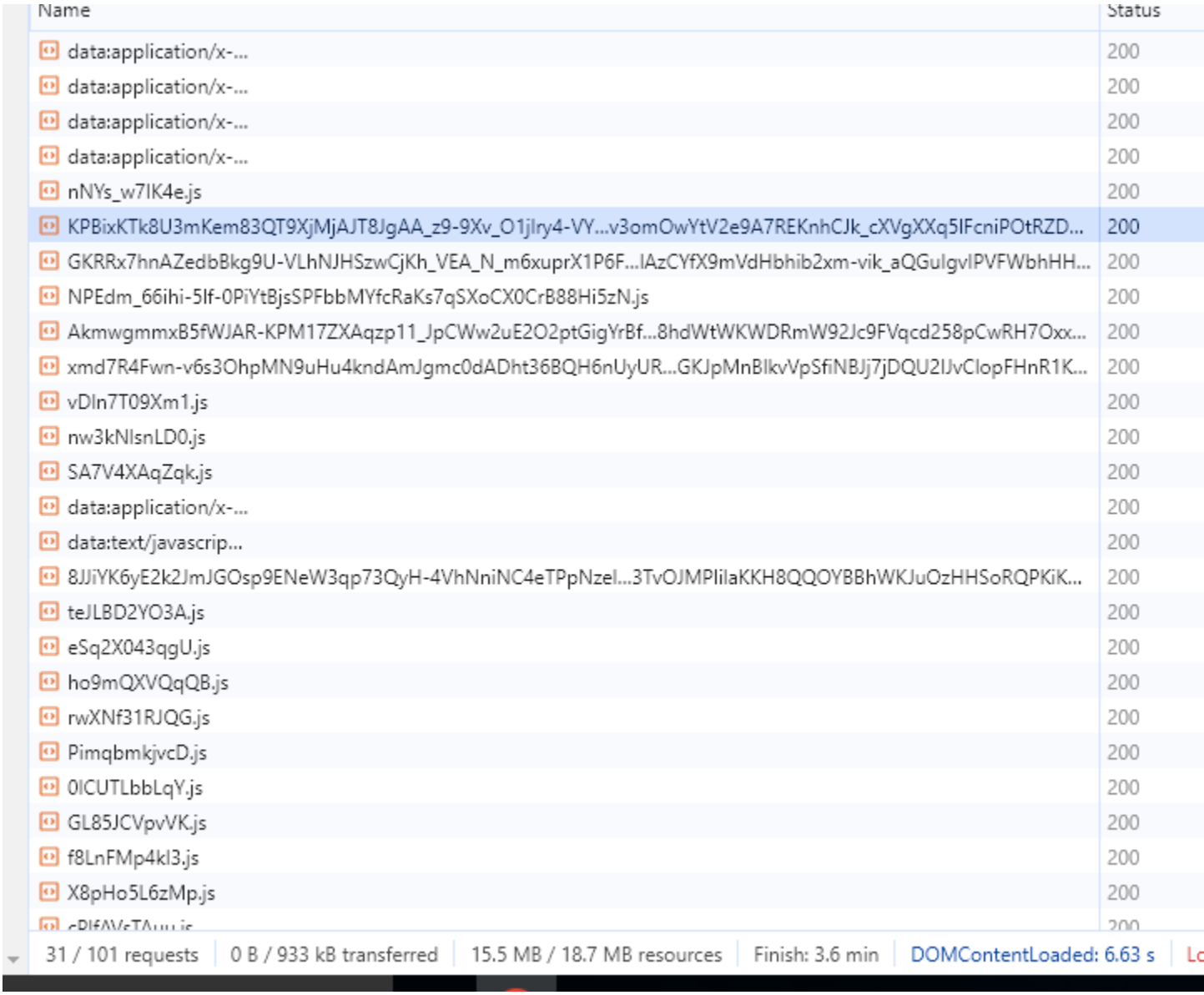


Andando poi ad aprire la steruttura dei Raw Headers, viene mostrata la “pistola fumante”:

Il metodo ha fatto sì che si venisse esposti alle richieste di “click.convertkit-mail2.com” in modo che l’indirizzo remoto potesse immagazzinare le informazioni.

L'anomalia più critica risiede nei file JSON scaricati dalla pagina. È stato identificato il modulo `UFICommentFileInputAcceptValues` , configurato in modo sospetto per accettare un vasto spettro di file:

- Documenti: `.pdf`, `.msword`, `.xlsx`.
- Media: `.mp4`, `.mkv`.



Verdetto Analitico: L'architettura non si limita al furto di password. L'interfaccia è strutturata per operare in ottica di *Data Theft* (furto di documenti aziendali o d'identità) oppure per attacchi di *Second-Stage Delivery*, inducendo la vittima a scaricare o caricare file infetti.

4. Azioni di Remediation e Mitigazione

Poiché l'endpoint non è stato compromesso da un eseguibile, le classiche difese basate su Antivirus/EDR non sono l'obiettivo primario. Le contromisure devono operare a livello di **rete**, **identità** e **consapevolezza**.

4.1 Remediation Immediata (In caso di click o inserimento dati)

- **Gestione Credenziali:** Forzare il reset immediato della password per gli utenti coinvolti.

- **Revoca Accessi (Cruciale):** Poiché l'attacco abusa del protocollo OAuth, cambiare la password potrebbe non bastare. È obbligatorio accedere alle impostazioni di sicurezza dell'account e revocare tutte le "Applicazioni di terze parti" e le sessioni attive sospette.
- **Monitoraggio:** Ispezionare i log aziendali alla ricerca dell'URL iniziale (`click.convertkit-mail2.com/...`) per identificare "Pazienti Zero" che hanno cliccato il link.

4.2 Mitigazione Strutturale (Prevenzione)

- **Filtraggio di Rete (Blacklisting Mirato):** Non inserire in blacklist l'intero dominio `click.convertkit-mail2.com`, in quanto servizio legittimo che bloccherebbe comunicazioni marketing valide. Implementare invece un blocco a livello di proxy Web/URL filtering esclusivamente sull'identificativo della campagna compromessa: `*/wvuqovqrrwagh50ndddc7hnxdlxxxu8/*`.
- **Hardening dell'Identità:** Implementare l'Autenticazione a Due Fattori (MFA), preferibilmente basata su standard resistenti al phishing come le chiavi hardware FIDO2.
- **Security Awareness:** Addestrare il personale a non fidarsi esclusivamente dei lucchetti HTTPS o della grafica di un sito, ma a ispezionare criticamente gli URL completi e a diffidare da richieste anomale di caricamento documenti su portali di login.

5. Regola YARA (Analisi File ed Email)

Questa regola è progettata per scansionare file `.eml` (email grezze) in ingresso nei gateway di posta, proxy log testuali o dump di memoria, alla ricerca della specifica catena di reindirizzamento:

```
rule Phishing_ConvertKit_OAuth_Abuse {
    meta:
        description = "Rileva la stringa URL malevola della campagna di Consent Phishing veicolata tramite ConvertKit"
        author = "Bkm4ge / Il Mago Nero"
        date = "2026-02-24"
        threat_type = "Credential Harvesting / OAuth Abuse"
        severity = "High"

    strings:
        // Dominio legittimo abusato come redirector
        $domain = "click.convertkit-mail2.com" ascii wide

        // Identificativo univoco della campagna ostile estratto dall'analisi
        $campaign_id = "wvuqovqrrwagh50ndddc7hnxdlxxxu8" ascii wide

        // Payload target codificato in Base64 (www.instagram.com/aussienurserecruiters)
        $b64_target = "d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2llbnVyc2VyZWNydWl0ZXJz" ascii wide
```

```
    condition:
        // L'innesco richiede la presenza congiunta del dominio e dell'ID campagna
        $domain and $campaign_id and $b64_target
}
```

5.2. Query SIEM (Analisi Telemetria di Rete)

Queste istruzioni logiche sono formattate per l'ingestione nei principali *Security Information and Event Management* (SIEM) per interrogare i log proxy, DNS o Firewall. L'azione si focalizza sul tracciamento degli endpoint interni che hanno generato traffico verso l'URL infetto.

5.3 Splunk (SPL)

Ricerca trasversale sugli indici di rete per isolare le transazioni web in uscita.

```
index=proxy OR index=firewall sourcetype=pan:threat OR sourcetype=squid
| search url="*click.convertkit-mail2.com/wvuqovqrrwagh50ndddc7hnxdlxxxu8*"
| stats count min(_time) as first_seen max(_time) as last_seen by src_ip, user, url, action
| convert ctime(first_seen) ctime(last_seen)
```

5.4 Microsoft Sentinel / Defender (KQL)

Interrogazione ottimizzata per le tabelle di eventi di rete e proxy aziendali.

```
DeviceNetworkEvents
| where RemoteUrl contains "click.convertkit-mail2.com"
    and RemoteUrl contains "wvuqovqrrwagh50ndddc7hnxdlxxxu8"
| project TimeGenerated, DeviceName, LocalIP, RemoteIP, RemoteUrl, ActionType
| sort by TimeGenerated desc
```

5.5 Elastic Security (Kibana / Lucene)

Filtro booleano per l'isolamento dei pattern all'interno dell'infrastruttura ElasticCS (ECS).

```
url.domain: "click.convertkit-mail2.com" AND url.path: *wvuqovqrrwagh50ndddc7hnxdlxxxu8*
```

6. Conclusioni e Valutazione di Sintesi

L'analisi dinamica e strutturale condotta sul task ha permesso di confutare in modo categorico l'ipotesi iniziale di un'infezione da "Agent Tesla". Le evidenze raccolte certificano l'assenza di compromissione a livello di host: non vi è stata alcuna inoculazione di file eseguibili, dropper o meccanismi di persistenza sul file system locale.

La minaccia è stata formalmente riclassificata come una **Campagna di Phishing Avanzato (Credential Harvesting e potenziale OAuth Abuse)**. Il vettore d'attacco si distingue per un elevato grado di sofisticazione architetturale, basato su:

1. **Abuso di infrastrutture legittime:** L'impiego del redirector `click.convertkit-mail2.com` garantisce l'elusione dei Secure Email Gateway (SEG).
2. **Mimesi applicativa:** Il traffico di rete non punta a server ostili, ma sfrutta domini certificati (`www.instagram.com`, `www.facebook.com`) per conferire legittimità visiva e crittografica alla pagina di atterraggio.
3. **Capacità asimmetriche:** L'analisi del payload JSON ha rivelato che la landing page è equipaggiata con moduli per il caricamento silente di documenti (Data Theft), esponendo l'organizzazione non solo al furto di identità, ma anche all'esfiltrazione diretta di dati sensibili.

In virtù di questi parametri sistemici, la strategia di difesa deve abbandonare il paradigma tradizionale *endpoint-centrico* (Antivirus/EDR) in favore di un approccio *identity-centrico*. La neutralizzazione della minaccia impone la revoca immediata delle sessioni e dei Token OAuth potenzialmente compromessi, parallelamente all'implementazione di regole di blocco perimetrale (Proxy/SIEM) calibrate esclusivamente sull'identificativo di campagna individuato, al fine di preservare il traffico di rete fisiologico.