S5.L2 OSINT/MALTEGO/Google Dorks

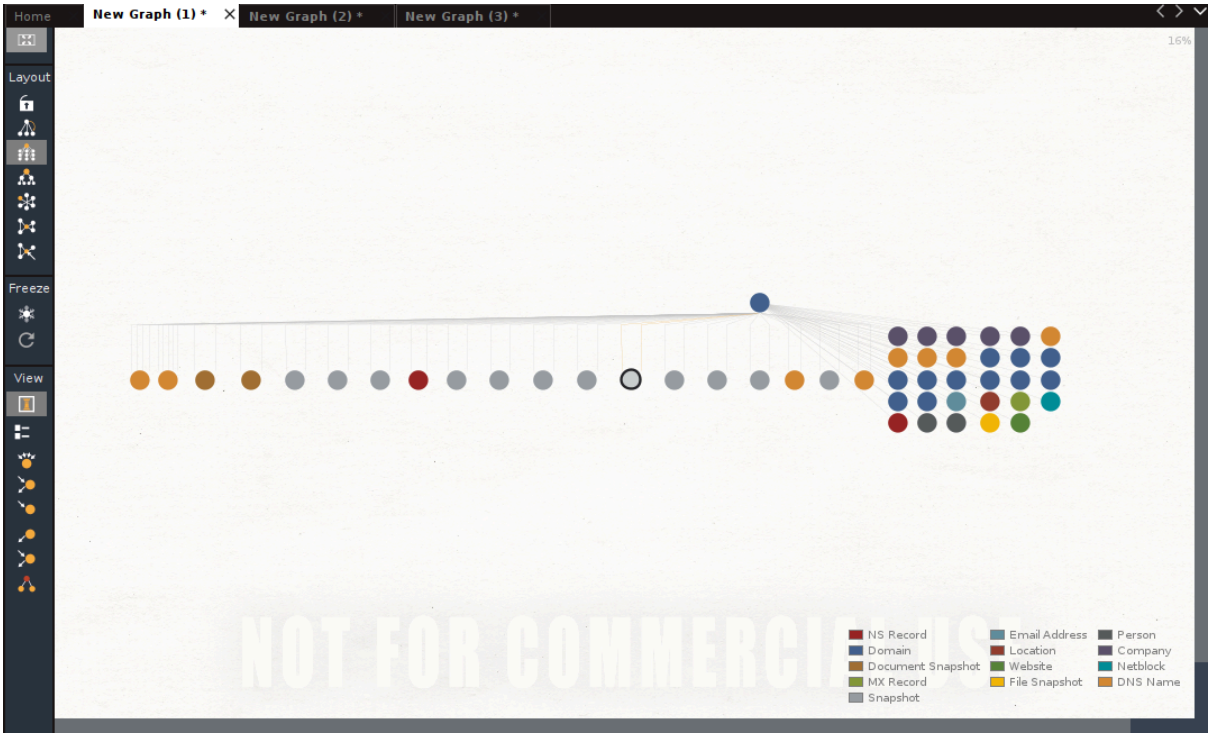
L'immagine seguente mostra un grafico di Maltego, che è stato utilizzato per eseguire un'analisi OSINT (Open Source Intelligence) sul dominio epicode.it. Vediamo cosa è stato fatto e come funziona questa analisi:

Cosa è Stato Fatto

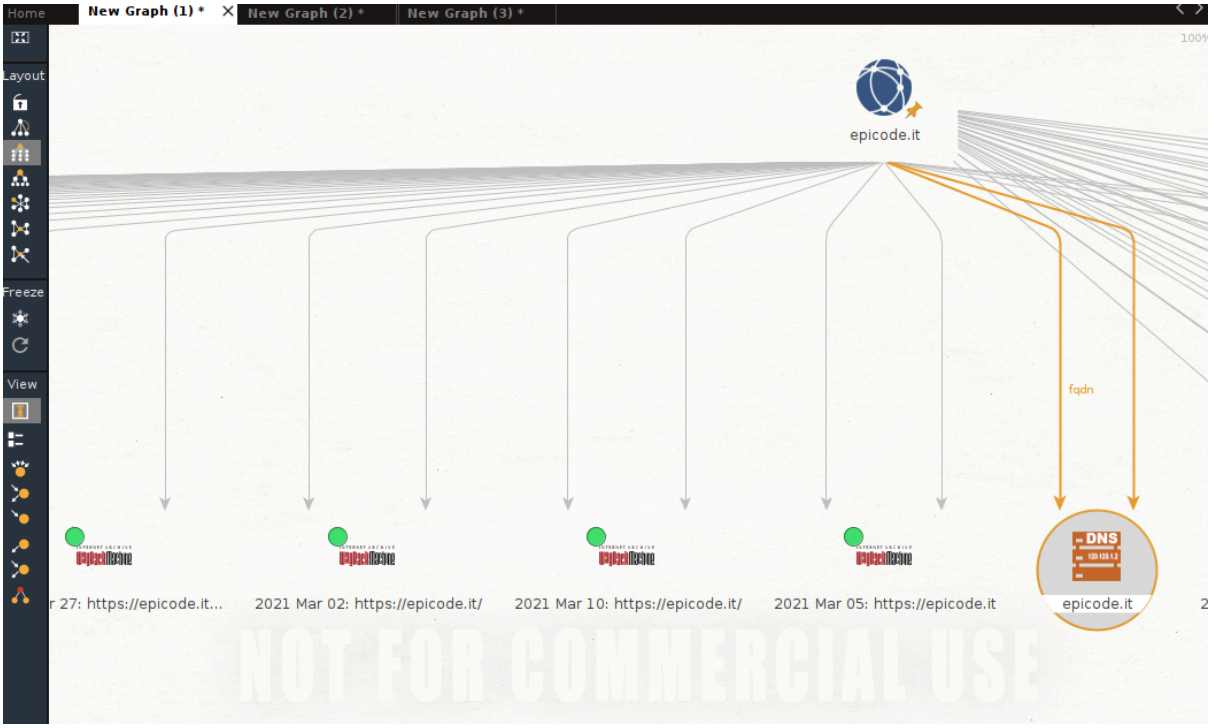
1. Inserimento del Dominio: Ho inserito "epicode.it" come dominio di partenza per il mio grafico in Maltego.
2. Espansione delle Entità: Utilizzando varie trasformazioni in Maltego, ho espanso il dominio per estrarre e visualizzare diverse entità collegate a questo. Queste entità includono record DNS, indirizzi email, documenti, snapshot di file, e altre risorse online correlate al dominio.

Perché L'ho Fatto

- Analisi della Sicurezza: Per identificare vulnerabilità potenziali o configurazioni errate nel dominio.
- Intelligence Competitiva: Per raccogliere informazioni su come epicode.it è strutturato online, quali tecnologie usa, e possibili partner commerciali o tecnici.
- Indagine Forense: Per raccogliere informazioni in caso di incidenti di sicurezza o violazioni dei dati riguardanti epicode.it.
- Ricerca di Mercato: Per comprendere meglio la presenza online di epicode.it e la sua rete di contatti e servizi associati.



Questo è il grafico delle ricerche effettuate al dominio epicode.it, adesso vediamo più nello specifico le informazioni:



L'immagine mostra un'analisi dettagliata del dominio epicode.it, evidenziando diverse informazioni chiave e la loro interconnessione. Ecco una sintesi delle informazioni principali:

1. Snapshot del Dominio: Viene visualizzato il dominio principale epicode.it al centro del grafico, indicando che è il nodo centrale da cui derivano tutte le altre informazioni.
2. Record DNS: Sono visibili i record DNS associati al dominio, inclusi:
    - FQDN (Fully Qualified Domain Name): Mostra i nomi completi del dominio, che possono essere utilizzati per identificare host specifici all'interno del dominio epicode.it.
    - Indirizzi IP: Gli indirizzi IP associati ai server di epicode.it vengono visualizzati, essenziali per capire dove sono ospitati i servizi web e di email.
3. Timestamp: Alcuni nodi includono timestamp (es. "2021 Mar 02: https://epicode.it/"), che potrebbero indicare la data di cattura di specifici snapshot del sito o di cambiamenti significativi nelle configurazioni del dominio.

4. Altri Domini e Sotto-domini: L'analisi ha rilevato vari altri domini e sotto-domini collegati direttamente al dominio principale, suggerendo una possibile espansione o segmentazione dei servizi offerti da epicode.it (es. uso di differenti sotto-domini per servizi interni o esterni).
5. Connessioni di Rete: Le connessioni tra i vari elementi nel grafico indicano relazioni di rete e gerarchie all'interno dell'infrastruttura IT di epicode.it, utili per comprendere come il traffico dati è gestito e distribuito.

Queste informazioni forniscono un quadro tecnico dell'architettura di rete e della presenza online di epicode.it, utili per valutazioni di sicurezza, audit tecnologici o analisi competitive.
procediamo con altre informazioni:

L'immagine illustra ulteriori dettagli tecnici e le connessioni di rete per il dominio epicode.it, svelando informazioni sulla struttura dei suoi sottodomini e affiliati, nonché le loro connessioni DNS. Ecco un'analisi tecnica degli elementi principali mostrati nel grafico:

1. Organizzazioni e Affiliazioni:
    - WeCode Srl e 1 Api GmbH sono evidenziate come organizzazioni connesse, potenzialmente indicando una relazione contrattuale o di partnership. WeCode Srl potrebbe essere un'entità commerciale o tecnologica che collabora con epicode.it.

2. Infrastruttura DNS:
    - Vengono mostrati vari server DNS come ns81.domaincontrol.com e ns82.domaincontrol.com, che sono server di nome di dominio che gestiscono la risoluzione dei nomi per epicode.it e i suoi sottodomini.
    - dev1.colluado.epicode.it, learn.colluado.epicode.it, e dev2.colluado.epicode.it rappresentano sottodomini utilizzati presumibilmente per sviluppo, test e formazione.
3. Presenza Internazionale:
    - Sono presentati diversi domini geolocalizzati come epicode.us, epicode.cn, epicode.com.my, epicode.fr, epicode.gr, indicando una presenza globale o un targeting di mercati specifici in diverse regioni geografiche.
4. Dettagli Tecnici e Contatti:
    - L'icona dell'email dns@jomax.net potrebbe indicare il contatto tecnico o amministrativo per la gestione DNS.
    - Marco Rossi è mostrato con un'icona di persona, suggerendo che può essere un contatto chiave o un responsabile tecnico.
    - Il nodo con "JSON" e "2021 Sep 22: default.json" indica la presenza di un file di configurazione o di dati in formato JSON, utilizzato in una specifica data.
5. Indirizzi IP e Mail Server:
    - Gli indirizzi IP come 93.95.216.84 e 93.95.216.84 sono elencati con il record MX, indicando i server che gestiscono il traffico di posta elettronica per epicode.it.
6. Ulteriori Domini e Sottodomini:
    - Domini come epicode.de, epicode.ai, e epicode.solutions suggeriscono un'espansione o una diversificazione nei servizi offerti, forse focalizzati su intelligenza artificiale, soluzioni tecnologiche, ecc.

Nel grafico, vediamo un assortimento di nodi colorati che rappresentano diverse tipologie di dati (come NS Record, MX Record, indirizzi email, ecc.), e linee che li collegano, indicando relazioni e connessioni dirette. Ogni colore rappresenta un tipo di dato specifico, facilitando l'identificazione visiva delle varie categorie di informazioni raccolte durante l'analisi. Questo aiuta gli analisti a comprendere rapidamente la struttura e le relazioni all'interno del dominio esaminato.

GOOGLE DORKS:

Google Dorks è una tecnica che utilizza query di ricerca avanzate per trovare informazioni specifiche sui siti web utilizzando Google. Questo metodo sfrutta i "dorks", che sono essenzialmente le query che includono operatori avanzati di ricerca di Google per filtrare risultati più dettagliati. Ecco alcuni esempi di Google Dorks che si possono usare per ricercare informazioni relative al dominio epicode.it**:**

1-File Specifici: Per trovare file specifici come PDF, docx, o xls ospitati sul dominio

site:epicode.it filetype:pdf
site:epicode.it filetype:doc
site:epicode.it filetype:xls

2-Informazioni sul Login: Per cercare pagine di login

site:epicode.it inurl:login

3-Configurazioni esposte: Per cercare file di configurazione esposti che non dovrebbero essere accessibili pubblicamente.

site:epicode.it ext:cfg | ext:conf

4-Errori e Messaggi: Per trovare pagine che contengono errori o messaggi di debug che potrebbero rivelare dettagli tecnici

site:epicode.it intext:"error" | intext:"warning" | intext:"not found"

5-Directory Listing: Per vedere se ci sono directory che vengono elencate senza restrizioni.

site:epicode.it intitle:"index of" | intitle:"directory listing for"

6-Documenti Riservati: Per cercare documenti che potrebbero essere riservati o sensibili.

site:epicode.it intext:"confidential" | intext:"restricted"

7-Informazioni Sui Dipendenti: Per cercare informazioni che potrebbero essere rivelate involontariamente su dipendenti o pratiche interne.

site:epicode.it intext:"email" | intext:"phone"

8-Versioni del Sito: Per trovare versioni precedenti o archiviate del sito.

site:epicode.it inurl:archive | inurl:old.

In conclusione:

L'OSINT, quando applicato correttamente, è uno strumento vitale per la protezione, l'analisi e l'intelligenza delle operazioni online. Google Dorks offre un metodo diretto per sondare informazioni specifiche attraverso la ricerca avanzata, mentre Maltego offre un'ampia visualizzazione delle reti e delle connessioni tra le entità raccolte. Insieme, queste tecniche permettono di ottenere una panoramica complessiva e dettagliata di un dominio, supportando una varietà di attività operative e strategiche.