3. Strumenti OSINT

FOCA

I metadati sono informazioni incorporate all'interno di un file, spesso invisibili all'utente durante il normale utilizzo. Sono definiti "data about data" poiché descrivono le caratteristiche del file, come il nome dell'autore, la data di creazione, la versione del software utilizzato per crearlo e altre informazioni tecniche. L'analisi dei metadati può fornire dettagli utili in contesti investigativi o per restringere il campo di indagine.

FOCA, acronimo di "Fingerprinting Organizations with Collected Archives", è uno strumento progettato per individuare ed estrarre metadati e altre informazioni nascoste dai documenti. Se questi file sono linkati a pagine web, FOCA può scaricarli e analizzarli per rivelare dettagli significativi. Funziona su sistemi Windows, Wine o su macchine virtuali, ed è disponibile sul sito ufficiale di ElevenPaths.

Tra le funzionalità principali di FOCA, c'è la capacità di effettuare ricerche automatizzate con motori come Google o Bing per identificare documenti di tipo Office (come .docx, .xlsx, .pdf) presenti su un determinato sito. Una volta scaricati, i file vengono analizzati per estrarre informazioni quali:

- Nome del creatore del file.
- Timestamp di creazione e modifica.
- Percorsi completi che includono nomi utente (ad esempio, `C:\Documents and Settings\Joe`).
- Versioni dei sistemi operativi e del software.
- Stampanti condivise e risorse di rete locali o remote.
- Nomi NetBIOS, hostname, indirizzi IP.
- Modelli di dispositivi mobili o fotocamere usati per generare i file.

Oltre all'analisi dei metadati, FOCA offre funzionalità avanzate che lo rendono uno strumento versatile anche in contesti di sicurezza informatica. Tra queste:

- Identificazione di vulnerabilità come SQL injection.
- Rilevamento di directory aperte o non protette.
- Esecuzione di trasferimenti di zona DNS.
- Analisi di metodi HTTP insicuri.
- Individuazione di file sensibili ("juicy files").

FOCA rappresenta quindi uno strumento potente sia per l'analisi dei metadati che per attività avanzate di auditing e sicurezza informatica, ma deve essere utilizzato con consapevolezza e responsabilità per evitare abusi.

Maltego

Maltego è un software avanzato sviluppato da Paterva che consente di raccogliere, analizzare e visualizzare dati pubblicamente accessibili in modo strutturato e grafico. Si basa sull'uso di "trasformazioni", ossia plugin che permettono di effettuare ricerche e creare correlazioni tra le informazioni disponibili. Sebbene non sia specificamente progettato per l'analisi delle reti sociali (Social Network Analysis, SNA), si concentra sulla link analysis, cioè lo studio delle connessioni tra i dati.

Il programma è disponibile in due versioni principali: la Community Edition, gratuita ma con alcune limitazioni, e una versione a pagamento con licenza annuale, che offre una gamma di funzionalità avanzate. La Community Edition permette agli utenti di sperimentare molte delle trasformazioni disponibili, mentre la versione commerciale consente un uso più esteso e integrato. Gli utenti della community possono anche contribuire con trasformazioni personalizzate, ampliando ulteriormente le potenzialità del software.

Maltego permette di esplorare dati relativi a persone, organizzazioni, domini e indirizzi IP, rappresentando graficamente le connessioni per facilitare l'analisi. Può essere integrato con plugin commerciali, come **Social Links**, che espandono le sue funzionalità per l'analisi di dati provenienti da social network, piattaforme di messaggistica e altre fonti corporate.

Social Links è un'estensione commerciale che aumenta la capacità analitica di Maltego, supportando l'analisi di dati da piattaforme come Facebook, Instagram, LinkedIn, Telegram e persino darknet, incluse oltre 30 forum e marketplace senza necessità di autenticazione. Integra risorse come CompaniesHouse e OCCRP, ed è compatibile con strumenti di terze parti quali Shodan, SecurityTrails e Bitcoinwhoswho, permettendo un'analisi dettagliata anche nel campo delle criptovalute.

Gestendo un database di oltre 7 terabyte contenente e-mail, alias, nomi e numeri di telefono, Social Links consente operazioni complesse come il tracciamento di criptovalute, l'analisi di forum darknet e la raccolta di dati da documenti e piattaforme social. Questo rende Maltego, combinato con strumenti come Social Links, una risorsa estremamente potente per investigazioni OSINT, analisi forensi e monitoraggio della sicurezza informatica, risultando particolarmente utile per analisti e professionisti della sicurezza.

Paliscope

Paliscope è uno strumento avanzato progettato per facilitare le investigazioni online attraverso la raccolta di dati da fonti aperte (OSINT) in modo semplice, rapido e sicuro. La piattaforma consente di gestire l'intero flusso investigativo, dalla raccolta alla presentazione dei risultati. Con Paliscope è possibile acquisire automaticamente informazioni da siti web, social media, forum e altre fonti online, garantendo un’organizzazione ottimale dei dati raccolti e la loro analisi approfondita.

Grazie alle sue funzionalità, permette di identificare connessioni tra informazioni e soggetti, generando rappresentazioni grafiche utili per comprendere le relazioni. Inoltre, il software è progettato con particolare attenzione alla sicurezza, garantendo protezione e privacy durante tutte le fasi dell'investigazione. Per concludere le analisi, Paliscope offre la possibilità di creare report dettagliati e professionali, utili per documentare e comunicare i risultati ottenuti.

Questo strumento si rivela particolarmente utile in ambiti come le investigazioni forensi, il monitoraggio di attività sospette online, l'analisi di social media e la ricerca su darknet e marketplace digitali. L'interfaccia intuitiva e le funzionalità avanzate lo rendono ideale per chi opera nel campo investigativo e necessita di un approccio strutturato e professionale alle analisi di dati OSINT.

Geolocalizzazione

La geolocalizzazione è una tecnica fondamentale nelle investigazioni online, poiché consente di determinare il luogo fisico da cui un soggetto interagisce con una rete, come Internet o una rete mobile. Identificare una posizione geografica può rivelarsi cruciale per contestualizzare un'attività, verificare un'identità o raccogliere prove.

Strumenti come Infosniper permettono di inserire un indirizzo IP e ottenere una stima della posizione geografica associata, visualizzandola su mappe come Google Maps, Yahoo Maps o Microsoft Maps. Gli indirizzi IP utilizzati per la geolocalizzazione possono essere estratti, ad esempio, dagli header delle email o dai log dei siti web.

Creepy, un altro strumento interessante, consente di individuare la posizione geografica di un soggetto analizzando dati provenienti da social network come Twitter o esaminando i metadati delle immagini pubblicate su piattaforme come Flickr o Instagram. Questo software, disponibile su piattaforme come GitHub, sfrutta le informazioni contenute nei metadati per tracciare una localizzazione accurata, se presente.

Oltre agli strumenti software, esistono metodi non convenzionali per raccogliere dati geolocalizzati. Google Street View, foto satellitari o strumenti come Google Maps ed Earth permettono di esplorare abitazioni, aziende e dintorni, aggiungendo contesto alle informazioni raccolte. Anche i video pubblicati su piattaforme come YouTube o Vimeo possono contenere indizi geolocalizzabili, come ambientazioni specifiche riconoscibili.

Un metodo interessante e meno noto è l'analisi di un IBAN, che può rivelare informazioni sulla banca e, in alcuni casi, sulla posizione geografica associata. Strumenti online come Mutuissimo o IBAN Calculator permettono di decifrare le informazioni di un IBAN, inclusa la località della banca.

La geolocalizzazione, combinando strumenti tecnici e metodi creativi, fornisce una visione più ampia e dettagliata del contesto geografico associato a un soggetto o un'azione online, rappresentando un elemento chiave nelle investigazioni digitali.

Fake Profile

Un "fake profile", noto anche come "sock puppet", è un falso profilo o una falsa identità creata per diversi scopi. La chiave per un fake profile efficace è la plausibilità. Questo significa che deve essere progettato con attenzione, modellando le sue caratteristiche per risultare credibile e adatto al target specifico.

I fake profile vengono utilizzati per vari motivi. Possono servire per nascondere l'identità reale, per garantire la sicurezza propria o altrui, per assumere l'identità di un'altra persona, per creare confusione, per ottenere accesso a gruppi specifici o per manipolare il contesto in cui operano. Tuttavia, è fondamentale prestare attenzione all'uso di questi profili, poiché potrebbero sfociare in reati come la sostituzione di persona, regolata dall'articolo 494 del Codice Penale.

Diversi soggetti possono utilizzare fake profile, tra cui giornalisti, investigatori, analisti OSINT, agenzie governative e anche malintenzionati come stalker, cybercriminali o spammer. Gli esempi storici includono l'uso di sock puppets per influenzare l'opinione pubblica durante elezioni in Corea del Sud, Stati Uniti e Italia, o per infiltrarsi in organizzazioni e screditarle, come nel caso del "Team Themis".

Per costruire un fake profile efficace, è necessario definire con precisione il "personaggio", includendo dettagli come sesso, nome, storia personale, presenza sui social network, contatti, professione e altri elementi che lo rendano credibile. Se si tratta di un profilo aziendale, si possono aggiungere informazioni relative a prodotti, clienti e contatti aziendali.

Creare e mantenere un fake profile comporta rischi significativi. Il profilo può essere facilmente "bruciato" se non è coerente, e c'è sempre il rischio di esporre accidentalmente informazioni personali reali. In caso di scoperta, ci si espone a discredito personale o organizzativo, e ad altri rischi correlati.

Individuare fake profile richiede attenzione ai dettagli. Esaminare le foto postate (magari verificandole con strumenti come TinEye), valutare la frequenza di aggiornamento del profilo, controllare la lista degli amici, analizzare le informazioni personali come scuola o lavoro, e verificare la data di nascita sono strategie utili. Anche i post e i commenti possono rivelare incongruenze.

Molti fake profile sono generati automaticamente, spesso per attività di intelligence, marketing o disinformazione. Social network come Facebook stimano la presenza di milioni di profili duplicati. Esistono anche strumenti online per generare fake profile, come DataFakeGenerator, FakeNameGenerator e altri, che forniscono nomi, foto e dettagli fittizi per creare identità false. Tuttavia, il loro uso deve essere sempre ponderato e consapevole per evitare conseguenze legali o etiche.

Strumenti utili

Ecco una panoramica dei software e strumenti utili in ambito OSINT, con un focus sulle loro funzionalità principali e possibili applicazioni:

XMIND è uno strumento di mind mapping professionale e molto popolare, utile per organizzare e visualizzare idee, piani di ricerca e collegamenti tra informazioni.

FOCA è un software progettato principalmente per analizzare documenti alla ricerca di metadati e informazioni nascoste, che possono rivelare dettagli come versioni software, timestamp e percorsi dei file.

MALTEGO è una piattaforma versatile per la raccolta e l'analisi di dati, che consente di rappresentare visivamente le connessioni tra entità. Può essere potenziato con plugin come **Social Links**, utile per analizzare dati da social network, messaggistica e altre fonti.

CREEPY è uno strumento di geolocalizzazione che raccoglie informazioni geografiche da social network e dai metadati di immagini, fornendo un'analisi delle posizioni legate a un soggetto.

EXIF VIEWER è un componente aggiuntivo per Firefox che permette di visualizzare i dati Exif e IPTC nelle immagini JPEG, utili per estrarre informazioni come modelli di dispositivi, date e luoghi.

TOR BROWSER consente una navigazione anonima sfruttando la rete TOR, ideale per proteggere la privacy e nascondere la propria posizione durante le attività OSINT.

PALISCOPE è uno strumento per la raccolta e l'organizzazione di dati OSINT, pensato per supportare investigazioni dettagliate e creare report strutturati.

HUNCHLY è un altro software OSINT che facilita la raccolta e il tracciamento di informazioni durante ricerche online, offrendo strumenti per organizzare e analizzare i dati raccolti.