I VANTAGGI INVESTIGATIVI DI UN SISTEMA AVANZATO PER L'ANALISI DEL TRAFFICO DATI NELL'AMBITO DELLA LAWFUL INTERCEPTION

La diffusione di internet nelle telecomunicazioni impone un nuovo approccio tecnologico ed investigativo volto ad evidenziare e valorizzare in maniera integrata ogni tipo di metadato. Piattaforme di Telematica Passiva avanzate assumono quindi una centralità maggiore rispetto al passato in combinazione con altri strumenti più tradizionali.

Ing. Fabio ROMANI, Amministratore Delegato di IPS S.p.A., azienda leader a livello globale nel settore della Cyber Intelligence. I sistemi di IPS sono in esercizio in oltre 30 paesi del mondo, supportando ogni giorno centinaia di Forze di Polizia e Agenzie di Intelligence.
Dott. Yassine FATAH, Product Specialist di IPS S.p.A. e docente del dipartimento IPS Academy che ogni anno eroga più di cento giorni di formazione tecnica avanzata a decine di migliaia di operatori del settore.

L'analisi del traffico dati, in tutte le sue accezioni, ha sempre avuto un ruolo marginale tra le tecnologie utilizzate a supporto delle attività investigative.
Storicamente questo tipo di analisi non sempre ha fornito risultati soddisfacenti, a causa di una costante riduzione di risorse in ricerca e sviluppo da parte delle aziende del settore e dell'avvento di standard di cifratura sempre più avanzati. Queste due facce della stessa medaglia, insieme alla crescente diffusione dell'utilizzo dei captatori informatici, hanno reso di fatto l'analisi del traffico dati un mero accessorio tecnologico, apprezzato da pochissimi esperti, come supporto di altre tecnologie di intercettazione.

Considerando che con le attuali capacità computazionali si impiegherebbero decine di migliaia di anni per decifrare informazioni assicurate da TLS/SSL e chiave asimmetrica, la soluzione proposta dal captatore informatico è di fatto particolarmente interessante, a patto che se ne accettino anche i limiti, come la sua complessità o, nella maggior parte dei casi, l'esigenza di interagire con il target per poterlo convincere ad installare un'applicazione che si posizioni a monte della cifratura.

L'utilizzo del captatore, per le ragioni appena evidenziate, non è sempre possibile e sarà sempre più difficile in futuro; ciò a causa di diversi fattori: in primis gli investimenti di Google e Apple in sicurezza per rendere i propri sistemi operativi sempre più impenetrabili, a questo si aggiungono le complessità date dalla rivelazione delle metodologie di infezione utilizzate, infine il quadro normativo lascia delle zone opache che rendono questa tecnologia difficilmente utilizzabile a fini probatori.

A partire da queste considerazioni, **il presente articolo intende descrivere l'importanza di considerare i giusti strumenti di analisi del Traffico Dati durante tutte fasi di un' indagine**, ancor più se si tiene in considerazione che negli ultimi anni tutte le comunicazioni si sono spostate su Internet, non solo le chiamate di tipo *WhatsApp* ma anche le tradizionali chiamate oggi viaggiano su protocolli IP (es. VoLTE) e con l'avvento del 5G ogni tipo di comunicazione tra persone e/o tra dispositivi (IoT) utilizzerà la rete Internet.

Così come in certi contesti è più sicuro ed efficiente osservare l'attività di un soggetto di interesse, carpendo dall'esterno le informazioni che egli stesso ci concede, piuttosto che accedere nella sua dimora per mettersi in ascolto delle sue conversazioni, allo stesso modo **può essere preferibile rimanere passivi rispetto all'attività del target**, ma sempre e costantemente in ascolto, in attesa di cogliere le molteplici vulnerabilità a cui la navigazione Internet espone ognuno di noi, compreso il target.

A titolo d'esempio ponendo il focus sui servizi di messaggistica istantanea, nell'ambito del costante lavoro di ricerca e sviluppo dell'analisi del flusso dati telematico, emerge che durante l'utilizzo di tali servizi, molte informazioni di questi eventi possono essere raccolte con un lavoro euristico avanzato di estrazione metadati. Attraverso un meccanismo complesso ed automatizzato è possibile produrre un tabulato delle "attività social", riconducibile ai molteplici servizi di messaggistica istantanea presenti sul mercato che prevedono la possibilità di effettuare chiamate VoIP.

Tale tabulato è composto da diversi elementi:
- applicazione utilizzata (*WhatsApp, Telegram, Facebook, ecc.*);
- tipologia evento (chiamata vocale, videochiamata, messaggio, ecc.);
- durata evento;
- data e ora;
- identificativo univoco del target;
- identificativo univoco dell'interlocutore;
- ISP dell'interlocutore.

Da quanto sopra si evince che l'analisi del flusso dati può fornire informazioni di valore sul target, ma anche su tutti i soggetti ad esso collegati, ossia che interagiscono con il dato principale analizzato.

Si evidenzia di seguito il percorso dei dati, prima di un messaggio testuale, poi di un evento di tipo chiamata.

Messaggio testuale

1. Invio di testo dal telefono A verso il telefono B.
2. Il messaggio raggiunge il server del provider.
3. Il messaggio viene indirizzato verso il telefono B.
4. Il telefono A riceve conferma di ricezione e lettura da parte del server.
5. Il processo riparte in direzione opposta in caso di risposta del dispositivo B.

Figura 1 - Percorso dei dati di un messaggio testuale

In caso di intercettazione del traffico del dispositivo A, troveremo traccia di una serie di connessioni e metadati verso i server del provider.

Chiamata

Il percorso di un evento di tipo chiamata segue una strada diversa, riassunta come segue:

1. Tentativo di chiamata del dispositivo A verso il dispositivo B.
2. L'impulso raggiunge il server, il quale instrada il tentativo di chiamata al dispositivo B.
3. Il dispositivo B, in caso di risposta, instaura una comunicazione diretta con il dispositivo A.

si riescono ad evidenziare diversi metadati di interesse.
Le informazioni estratte con i rispettivi identificativi, sono sufficienti, congiuntamente con l'orario, a poter determinare il dispositivo in uso all'interlocutore della chiamata a mezzo social. Queste informazioni vengono dunque utilizzate per ricostruire identità e localizzazione di un soggetto di interesse.

L'arricchimento degli "identificativi" estrapolati dal traffico con i CDR (Call Detail Records) permette una più puntuale identificazione dei soggetti coinvolti. Il sistema sarà quindi in grado di presentare in griglia parametri come:

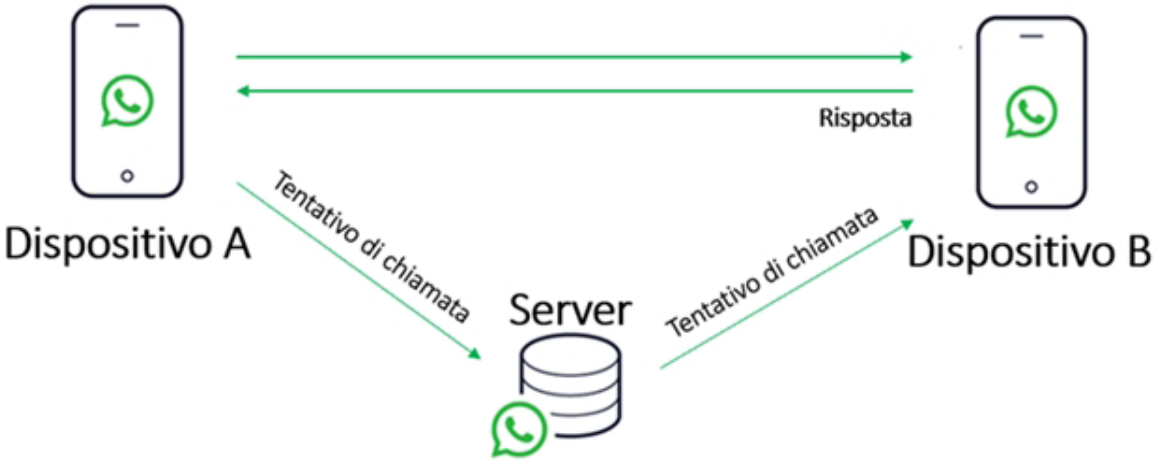

Figura 2 - Percorso dei dati di una chiamata

Il flusso che si instaura tra i due terminali è sicuramente più efficiente in termini di carico di lavoro per i server del provider, anche dal punto di vista della qualità della telecomunicazione. In questo quadro, conoscendo le logiche della comunicazione fra i due dispositivi

- Utenza Telefonica,
- Intestatario,
- IMSI,
- IMEI,
- Cella Telefonica agganciata al momento della chiamata.

I risvolti investigativi sono innumerevoli. Tramite questa tecnologia, infatti, si può associare una conversazione captata tramite intercettazione ambientale a due entità certe e certificate dal gestore telefonico che effettua il rigiro del flusso dati verso il server in Procura. Allo stesso modo si può avere contezza della destinazione delle comunicazioni da e verso l'estero effettuate tramite applicazioni considerate sicure da un sospetto terrorista o potenziale appartenente ad un'organizzazione criminale internazionale.

Ci sono alcuni concetti chiave che andrebbero considerati nel difficile computo dei costi benefici; l'intercettazione telematica passiva, a listino in ogni Procura della Repubblica, è una tecnologia da una parte trasparente nei confronti del target, il quale non potrà mai avere alcun tipo di sospetto circa un'eventuale indagine a suo carico (almeno dal punto di vista dell'interazione diretta), dall'altra assicura l'inconfutabilità ai fini probatori, in quanto il flusso dati viene garantito da un ente terzo quale il gestore telefonico.

Il sistema per la gestione della Telematica Passiva fornito da IPS, GENESI® IP Analyzer, si basa su una tecnologia in grado di supportare molteplici usi operativi, anche non tradizionali. Infatti, può essere utilizzato anche in modalità offline per importare e analizzare dump di traffico raccolti in diverse modalità (ad esempio, attraverso operazioni di tipo tattico, "sniffando" il traffico dati di una rete Wi-Fi; tramite l'utilizzo di una sonda; impiegando dump provenienti da altri sistemi di intercettazione in uso presso le varie Procure).

Nell'ambito della telematica passiva, si sottolineano gli indubbi vantaggi per le attività investigative derivanti da alcune funzionalità rilevanti di questo tipo di intercettazione, come ad esempio:

- Identificare quanti e quali dispositivi sono connessi ad una determinata rete. Ciò è spesso determinante sia dal punto di vista operativo per valutare l'ingresso o meno in un edificio con lo scopo di installare periferiche ambientali, sia a livello strettamente investigativo per comprendere se un'utenza mobile viene utilizzata come hotspot per altri dispositivi;
- Rilevare i server delle applicazioni e dei servizi contattati dagli utilizzatori della rete posta sotto intercettazione per produrre evidenze relative alla visita di uno specifico *hostname*;
- Comprendere la destinazione delle comunicazioni nazionali ed estere effettuate, fino a localizzare il target; mostrando anche le connessioni dello stesso target, grazie ad una comprensiva e immediata analisi delle relazioni;
- Tracciare il traffico di *upload* o *download* verso un determinato servizio (ad esempio, un forum web o YouTube) per individuare potenziali target (il riferimento è a coloro i quali inseriscono contenuti sulla rete per fenomeni di proselitismo e propaganda estrema, pedopornografia, diffamazione, atti persecutori, ecc.).
- Rilevare fasi di identificazione e metadati univoci legati a target utilizzatori di distribuzioni custom di sistemi operativi tipiche dei Crypto Phone (ad esempio, le oramai tramontate EncroChat, Sky ECC, e le più recenti Diamond Secure, No1BC, ...)

Tale elenco, non esaustivo, dimostra l'utilità di questo strumento investigativo, soprattutto quando affiancato ad altre tecnologie, come le intercettazioni telefoniche e del VoLTE, in un'ottica di analisi integrata. Il sistema di IPS, attualmente disponibile presso gran parte delle Procure della Repubblica, è utilizzato quotidianamente da diversi reparti investigativi su tutto il territorio nazionale, e tra l'altro è stato scelto come sistema di riferimento per l'analisi del traffico dati da parte di diverse articolazioni del Ministero dell'Interno.

Nel mondo delle telecomunicazioni, in continua evoluzione, internet sta assumendo un ruolo sempre più centrale. Questo è il motivo per il quale, oggi, non si può prescindere dall'utilizzo di uno strumento come quello descritto, fondamentale per qualsiasi attività investigativa. ©