Peculiarità delle perquisizioni dirette alla ricerca di evidenze informatiche. Il mondo e-mail

Author : Pier Luca Toselli

Date : 28 Gennaio 2019

Terzo articolo dedicato alle peculiarità delle perquisizioni dirette alla ricerca di evidenze informatiche, che ho voluto dedicare alle operazioni immediatamente conseguenti a quella che abbiamo definito l'individuazione del target.

Accade sempre più spesso, fermo restando quanto già evidenziato nei precedenti articoli, che il "target" sia costituito da e-mail che possono assurgere a prova o anche solo, a mero indizio.

Ormai le e-mail sono utilizzate nei più diversi ambiti e il loro impiego a fini probatori è facilitato dall'errata percezione di scrivere qualcosa che si potrà "cancellare" o che "rimarrà" riservato. Al contrario l'e-mail è un contenitore ricco di elementi di prova e indizi pressoché inesauribile, tanto che potremo affermare che oggi non esiste indagine - anche solo per un "vediamo cosa si dicono, non si sa mai…" - che non vada a prendere in considerazione la corrispondenza e-mail al pari dei messaggi sugli smartphone. Le possibili casistiche di acquisizione e analisi forense di email[1] è sterminata. Altrettanto vero che quell'errata percezione che sia un mezzo totalmente sicuro e riservato spinge a scrivere qualsiasi cosa senza preoccuparsi delle conseguenze di ciò che si è scritto: quest'ultimo aspetto viene amplificato quando i due interlocutori, magari appartenenti a sistemi "giuridici" differenti, danno per scontato aspetti di tutela e riservatezza non universalmente riconosciuti o alla facilità di diffusione e replica di una email che una volta inviata diventa di fatto non più reversibile e incancellabile.

Ho già dedicato un precedente articolo sulle e-mail[2] relativo alla problematica - a mio modo di vedere tutt'ora irrisolta - dell'acquisizione di e-mail aperte/chiuse e alle conseguenti implicazioni sul piano processuale, che ha avuto il pregio di sollecitare il dibattito attorno a questa tematica che manca di precise soluzioni "legislative", tanto dal venir risolta quasi sempre in punto di "legittimità" dalla Corte Suprema di Cassazione, e non sempre con soluzioni univoche ed uni interpretative. Questa volta vorrei soffermarmi su alcuni aspetti peculiari concernenti le perquisizioni che vedono l'e-mail costituire l'oggetto delle nostre attenzioni, senza pretesa di fornire una guida, ma piuttosto una serie di considerazioni pratiche che possono aiutare nella scelta dell'uno o dell'altro metodo per l'acquisizione forense delle e-

mail.

Problematiche nelle investigazioni sulle e-mail

Una delle prime problematiche legate alle e-mail che il digital forensics si trova a dover affrontare nel corso della perquisizione sono le credenziali necessarie ad accedervi. Lungi dall'essere banale e senza pretesa di esaustività potremo suddividere i probabili scenari operativi in due macro aree.

La prima è quella che permette di giungere sulla scena e rinvenire un dispositivo collegato e loggato sulla webmail o client e-mail utilizzato. Situazione, più probabile di quanto si possa pensare, atteso che il digitare ogni volta le proprie credenziali per accedere al client di posta o alla web mail alla lunga … stanca anche il più attento e smaliziato degli utilizzatori.

La seconda attiene al contrario a tutti quei casi in cui per giungere alle e-mail si necessitano delle credenziali (users e password), il cui ottenimento, è rimesso nel nostro ordinamento, a tecniche più o meno convincenti degli operatori di polizia, all'utilizzo di software sempre meno capaci di scovarle all'interno dei sistemi e per ultimo alla buona volontà della parte che è libera o meno di fornirle. Si arriva così al paradosso che in assenza di quest'ultime nulla si può se non il sequestro delle e-mail da notificare al provider con le difficoltà che ne derivano, qualora si tratti di notifiche da effettuarsi all'estero e per reati che magari non trovano accoglimento nei trattati di mutua assistenza. Invero anche il ricorso al cosiddetto "blocco" delle e-mail da parte dell'autorità giudiziaria, volto a preservare lo stato delle cose, ed effettuato attraverso il cambio delle "credenziali" e della catena di sicurezza legata alle stesse (doppia autenticazione, OTP One Time Password, etc.) risulta di fatto irrealizzabile se non si riesce ad accedere, almeno inizialmente, alle credenziali dell'utilizzatore.

Residuano quei casi relegati in prevalenza a situazioni particolarmente "fortunate" che vedono come già detto sopra l'utilizzo di alcuni software capaci, su alcune versioni di client, di indicare prontamente l'user e password utilizzata ad esempio con Mail PassView della NIRSOFT[3], viceversa l'individuazione di tali dati richiede l'effettuazione di operazioni tecniche di analisi che spesso mal si conciliano con i tempi e le modalità delle perquisizioni. Non si può escludere che con più approfondite ricerche si possa pervenire alla individuazione delle stesse, a file più o meno facilmente individuabili, contenenti le password utilizzate dal soggetto, o ancora che attraverso le stesse si possa pervenire alla realizzazione di una "libreria" di parole che potrebbe aiutare non poco in operazioni di "brute-force" volte all'individuazione della password utilizzata.

La raccolta di e-mail: quali strumenti utilizzare

Supponiamo di aver ottenuto anche le necessarie credenziali per accedere alla web mail o al client protetto e proseguiamo nella nostra disamina.

La seconda problematica è legata a due aspetti già evidenziati in precedenza, ovvero se il target è costituito da una web-mail (es. gmail, yahoo mail, libero mail, alice mail etc.) o se le

stesse sono scaricate e lette su di un dispositivo attraverso appositi client di posta e-mail (es. Outlook, Thunderbird, Mail etc.).

Volendo semplificare la differenza tra client di posta e web mail, potremo evidenziare che la web mail permette la gestione della posta elettronica direttamente sul browser, tramite l'interfaccia di posta elettronica del provider utilizzato, con il vantaggio di poterla gestire di fatto da qualsiasi dispositivo in grado di connettersi alla pagina web, per dirla meglio, per accedere alla propria casella di posta basterà raggiungere la pagina di login e accedervi tramite username e password.

Ad ogni buon conto, per quel che qui rileva l'eventuale acquisizione avverrà di fatto, dopo l'autenticazione, attraverso lo scarico della posta effettuato attraverso una connessione internet, che ovviamente in tali casi è indispensabile.

Il client di posta è invece uno specifico software scaricato e in funzione sul singolo dispositivo e che permette di gestire la lettura, l'invio e l'archiviazione delle e-mail direttamente dal desktop. Le e-mail sono memorizzate direttamente sul computer, e non è necessaria (salvo la necessità di una immediata sincronizzazione con il server) una connessione Internet, questo ovviamente comporta diversi vantaggi in capo al digital forensics.

Potremmo dire che qualora il soggetto utilizzi esclusivamente la webmail, il sequestro del PC o la bit-stream image dello stesso potrebbe permettere al più di leggere solo alcuni messaggi di posta o parte di essi ricostruiti attraverso gli artifacts che alcuni software riescono ad individuare durante il parsing, ma saremo ben lontani ovviamente dai risultati ottenibili attraverso lo scarico della web mail utilizzata o (quando si è fortunati) dalla presenza dei file di archiviazione del client di posta (es. il file .pst o .ost di Outlook).

Invero l'operatore di polizia qualora si riscontri l'utilizzo esclusivo di una web mail può essenzialmente operare attraverso tre tecniche:

- La prima consiste nell'accedere alla web-mail e laddove previsti, attraverso specifici tool (per es. nel caso di GMAIL – GOOGLE TakeOut), è possibile scaricare nel formato standard MBOX, tutte le mail catalogate con una certa etichetta o anche tutte le mail presenti, in questo esempio e caso in GMAIL. La procedura invero, prevede l'invio di un link al richiedente attraverso il quale provvedere allo scarico non solo delle e-mail ma anche di altri dati (spesso rilevanti) del profilo "Google" dell'utilizzatore quali rubrica, calendario etc. Ovviamente là è necessario effettuare il LOG e solo in seguito accedere ad una specifica procedura in termine alla quale si riceverà sull'indirizzo e-mail indicato durante il wizard (può essere lo stesso indirizzo e-mail che si sta scaricando ovvero un altro) il link per lo scarico che permetterà a sua volta di scaricare (e qui occorre fare attenzione alle performance della connessione e alla quantità di dati) uno o più file .zip contenenti le e-mail etichettate, tutte le mail presenti nell'indirizzo GMAIL target e/o gli altri dati relativi al profilo GOOGLE. Tale procedura a prima vista "diretta" e "comoda" difetta tuttavia di un controllo sui tempi necessari all'operazione, in quanto non esiste una barra di stato o altro che possa anche solo indicativamente fornire una tempistica all'operatore. Inoltre, da non sottovalutare il problema legato alle "credenziali". A

seguito dell'invio del link vengono nuovamente richieste le credenziali di accesso, ne consegue che per il completamento dell'operazione di "takeout" talvolta potrebbe rendersi necessaria un'operazione di "spossessamento" in capo al legittimo titolare delle credenziali ed una variazione di tutto l'apparato di "sicurezza" quali numero di cellulare associato al profilo (nel caso di sicurezza di secondo livello), modifica delle domande di sicurezza in caso di smarrimento della password etc. Al fine di impedire che nelle more delle operazioni di take out, che si ripete, si sa quando iniziano ma non si sa quando finiranno, il legittimo titolare possa modificare le credenziali di accesso, rendendo poi di fatto impossibile accedere ai file cui il link fa rimando. Accade infatti, che le FFPP al fine di portare a termine l'operazione di takeout procedono a modificare le password di accesso e gli step di sicurezza previsti da Google; senza entrare nel merito della legittimità e validità di tale procedura è innegabile come alla stessa si debba ricorrere talvolta, previo assenso dell'organo requirente, essendo l'unica operazione possibile, capace di garantire l'inalterabilità delle e-mail nelle "more" di effettuazione delle operazioni tecniche necessarie alla loro acquisizione;

- La seconda ed in alternativa, sempre nel caso che il target sia costituito da una webmail, è il ricorso all'utilizzo dei più comuni client di posta, attraverso i quali procedere allo scarico, previa autenticazione (sempre necessaria) e solo a scarico ultimato procedere attraverso il client alla esportazione in un file .pst (nel caso di Outlook) o .mbox. Invero client come Outlook permettono, a sincronizzazione avvenuta, di esportare tutta la posta in un file .pst di facile "gestione" dal punto di vista forense. Il file .pst può infatti poi essere facilmente esportato dopo essere stato compresso e sottoposto ad hasing. La compressione è una buona tecnica in quanto così facendo si impediscono inavvertite modifiche al file .pst, qualora poi lo stesso venga riaperto e ricaricato in fase di analisi attraverso Outlook stesso ed in ogni caso rappresenta: un'ulteriore salvaguardia all'integrità e immodificabilità del file; ed ancora vi è la possibilità di comprimere il file ed assicurarlo attraverso una password che va a costituire un ulteriore livello di "riservatezza" circa il contenuto del file. Anche qui va tuttavia precisato che il giusto innalzamento dei livelli di sicurezza da parte dei diversi provider ha fatto sì che, rispetto al passato, oggi tali operazioni richiedano al di là dei client e-mail utilizzati l'accesso alla web-mail e l'impostazione della stessa ad accettare "l'intervento" del client di posta scelto. In particolare ormai quasi tutte le web-mail chiedono espressamente all'utilizzatore titolare di autorizzare lo specifico client ad accedere alla web-mail, dopo aver autorizzato l'invio POP/IMAP. Ad ogni buon conto, ogni client ed ogni web mail presuppongono per farla breve una reciproca, specifica impostazione che oggi con l'innalzamento come si diceva dei livelli di sicurezza, non risulta sempre "automatica" e richiede l'intervento dell'utilizzatore/operatore per essere portata a buon fine. In ogni caso, in rete digitando la propria webmail e il client di posta che si intente utilizzare è possibile rinvenire molte guide che spiegano passo-passo come procedere. Preme qui in stretta connessione con l'argomento trattato richiamare l'attenzione quando si procede a tali configurazioni sulle profonde differenze tra i protocolli POP ed IMAP e relative conseguenze.

POP e IMAP come molti sanno, lavorano diversamente, con POP il programma si connette al server, recupera tutta la posta, la conserva in locale come nuova posta da leggere, cancella i messaggi dal server principale e si disconnette. Invero, ormai, nei client e nelle caselle di

posta che utilizzano POP, è prevista anche la possibilità al di là delle modalità di azione e cancellazione dei messaggi dal server di questo protocollo, di conservare comunque una copia dei messaggi anche sul server dopo il loro scarico in locale; tuttavia la caratteristica principale di POP rimane quella, (qualora non si preveda di preservarne una copia sul server remoto) di eliminare la posta dal server, che si traduce, nel non poterla più vedere se si accede al proprio account e-mail via browser da altri dispositivi.

Di contro usando IMAP il programma si connette al server di posta, richiede il contenuto dei nuovi messaggi e permette di visualizzarli sul dispositivo remoto salvandoli in cache, l'ovvia conseguenza è che l'utente legge il messaggio, lo modifica o la segna come letto, tali modifiche vengono recepite anche a livello server, ma in ogni caso il messaggio non viene rimosso dal server.

Il tutto per evidenziare che andrà posta particolare attenzione nell'utilizzo di POP allorquando il client utilizzato per lo scarico e la casella di posta non prevedano la conservazione di una copia del messaggio sul server remoto, essendo insito il rischio di "cancellare" dal server remoto i messaggi costituenti il nostro target, durante le operazioni di acquisizione dei messaggi.

- La terza possibilità è costituita dal ricorso a specifici programmi, alcuni dei quali "forensics-oriented". Qui il panorama invero si allarga tra programmi quali (per esempio) MailStore Home[4] e programmi più forensic-oriented quali AID4MAIL[5], in questa forchetta esemplificativa trovano posto anche molti altri prodotti (quale SECURECUBE IMAP DOWNLOADER[6]) tutti connaturati, comunque da una certa facilità di utilizzo e che sostanzialmente risultano anche accomunati dalle modalità di funzionamento consistenti, si perdoni la sintesi, nel collegarsi al server remoto (sempre previo superamento delle difficoltà già sopra evidenziate) e scaricare copia dei messaggi ivi presenti. Voglio ringraziare un consulente[7] che mi ha fatto conoscere eDiscovery Office 365[8]. Analogamente voglio ringraziare un altro consulente tecnico di informatica forense[9] che mi ha fatto conoscere Google Vault[10].

La differenza tra i vari prodotti è quasi sempre relegata alla:

- possibilità di ridurre considerevolmente i tempi di scarico e gestione della copia dei messaggi con modalità "forensi" che ne assicurino la genuinità, completezza ed inalterabilità/immodificabilità o per dirla breve, calcolo degli algoritmi di hash sui file scaricati;
- presenza nel software di barre di stato, o altri indicatori in grado quant'anche sommariamente di permettere una stima dei tempi necessari alle operazioni;
- facilità di utilizzo, presenza di Wizard, presenza di funzioni avanzate capaci di agevolare il collegamento al server remoto, possibilità di selezione dei soli messaggi di interesse allorquando il target risulti di facile ed immediata, individuazione.

La scelta di una o più, delle tre tecniche sopra elencate, è legata pertanto a diverse e numerose variabili che l'operatore di polizia dovrà tenere in considerazione, a titolo di mero riepilogo ne cito alcune, senza alcuna pretesa di esaustività e nella consapevolezza che quando leggerete questo articolo alcune saranno superate ed altre elemento di novità da risolvere. Ad ogni buon

conto evidenzio che solo l'esperienza e la pratica sul campo permettono di affinare nel tempo tali scelte in tempi rapidi e con effetti ottimali e … come esperienza insegna, ricordate sempre di annotare o meglio verbalizzare ogni vostra operazione così da poter sempre rammentare le operazioni svolte e poter giustificare le scelte operate:

- dimestichezza con i software a disposizione e le tecniche da adottare (i wizard non sempre sono una panacea);
- velocità della rete a disposizione: un takeout da 30 GB … fa invecchiare: tenente conto dei tempi non solo di gestione del takeout da parte di Google (tempi necessari alla predisposizione dell'archivio il cui link verrà inviato via email), ma anche dei tempi necessari allo scarico via rete dell'archivio, fermo restando come detto in precedenza che tale stima … non è facilmente quantificabile, anche se Google ha recentemente incrementato e velocizzato detto servizio;
- possibilità di limitare, restringere, focalizzare l'attenzione solo su alcune e-mail e non sull'intera casella di posta elettronica;
- possibilità di effettuare una stima dei tempi necessari all'effettuazione delle operazioni e valutare il ricorso su autorizzazione dell'organo requirente ad operazioni di "blocco" della casella e-mail da parte dell'intestatario/utilizzatore in attesa della loro acquisizione;
- verifica dell'utilità ai fini investigativi (de quo) degli archivi di posta già presenti in locale.

Alcune facilitazioni nella raccolta di email

Le cose risultano facilitate qualora il target sia costituito da un client e-mail ovvero quando l'utilizzatore, pur utilizzando una webmail utilizzi un client e-mail per la loro gestione, non avvalendosi esclusivamente degli strumenti "web" messi a disposizione dal provider.

Prendiamo per esempio un target costituito da messaggi e-mail gestiti dall'utilizzatore attraverso un client, "Outlook", tralascio qui di evidenziare le differenze tra i due tipi di files generati da detto programma ovvero files dati .pst e .ost, in rete si trovano centinaia di link dove troverete specificazioni tecniche e descrittive sul modo di funzionamento e sul contenuto dei files .pst e .ost. Preme invece in questa sede segnalare come agli stessi link che ne descrivono le differenze troverete anche le path o percorsi di detti files che risultano presenti "in locale" sul dispositivo del soggetto sottoposto a perquisizione che faccia uso di tale client. Orbene sulle tecniche di copia ed esportazione di detti files non mi sto a dilungare, salvo ribadire che al di là delle scelte di comodo ed operative di ciascuno dovrà essere assicurato il rispetto delle prescrizioni imposti dalla L.48/2008. Personalmente, a seconda degli scenari, tendo a prediligere l'utilizzo di FTK IMAGER LITE[11] o se si stanno utilizzando LIVE LINUX FORENSIC qualsiasi programma che ne permetta l'esportazione, calcolo dell'hash ed indicazione della path (ognuno ha i suoi prediletti – io personalmente per tali operazioni su singoli e pochi files non disdegno Dhash2 –Vers.2.0.1. che si trova in Deft0 – 2018[12], sia per la sua velocità che per la sufficiente e chiara reportistica).

Oltre a quanto finora evidenziato preme segnalare come qualora l'operatore si trovi dinanzi a particolari sistemi di gestione della posta (per es. Zimbra), client particolari (per es. Lotus Note), etc. sarà sempre bene avvalersi di ausiliari di P.G. all'uopo nominati[13], che potranno fornire le

necessarie credenziali ed assistenza finalizzata all'individuazione, esportazione ed acquisizione dei messaggi di posta.

Si segnala che ci sono profonde e sostanziali differenze tra gli utenti privati ed aziendali, nel senso che questi ultimi, per ragioni prevalentemente di riservatezza, sicurezza e gestione aziendale tendono prevalentemente ad utilizzare sistemi di gestione della posta maggiormente complessi e che presentano diversi livelli di sicurezza ed autenticazione che ne rendono più complesse le operazioni sopra descritte.

Rimandando ciascuno alla valutazione delle opportunità e potenzialità dei singoli strumenti sul piano delle investigazioni relative ad email soprattutto in ambito aziendale, si evidenzia come la conoscenza dei vari tool possa risultare talvolta strategica nella soluzione delle problematiche evidenziate.

Note

- [1] https://www.bit4law.com/laboratorio-informatica-forense/acquisizione-forense-email/
- [2] https://www.ictsecuritymagazine.com/articoli/email-aperta-email-chiusa-un-problema-tuttaltro-risolto/
- [3] https://www.nirsoft.net/utils/mailpv.html
- [4] https://www.mailstore.com/en/products/mailstore-home/
- [5] https://www.aid4mail.com/
- [6] http://securcube.net/it/securcube-imap-downloader/
- [7] https://www.linkedin.com/in/nbaldi
- [8] https://docs.microsoft.com/it-it/office365/securitycompliance/ediscovery
- [9] http://www.micheleferrazzano.it
- [10] https://gsuite.google.it/intl/it/products/vault/
- [11] https://accessdata.com/product-download/ftk-imager-lite-version-3.1.1
- [12] http://www.deftlinux.net/
- [13] https://www.ictsecuritymagazine.com/articoli/lintervento-dellausiliario-di-polizia-giudiziaria-ex-art-348-c-p-p-nelle-perquisizioni-informatiche/

Articolo a cura di **Pier Luca Toselli**