# Digital forensics e cyber security: caso Cellebrite Ufed vs Signal

Dal punto di vista tecnico-operativo, le indagini di *digital forensics* vengono svolte utilizzando specifici strumenti *hardware* e *software*[1] che, una volta collegati al sistema informatico da acquisire, ne esplorano le aree di memoria e ne producono una copia[2] – nella quale vengono ricompresi lo spazio non allocato e le parti di file cancellati ma non definitivamente eliminati – che successivamente viene esfiltrata verso un *file* di *backup* appositamente creato sul dispositivo *hardware* usato per l'acquisizione e dove viene, quindi, dislocata la copia forense del sistema sotto indagine. Concluse le operazioni di acquisizione, il clone informatico viene poi analizzato mediante programmi di analisi che permettono di prendere visione del contenuto digitale in esame. In particolare, questi *software* hanno il compito di scandagliare a fondo tutti i singoli file che sono presenti nella copia forense, visionandone tutte le parti, metadati inclusi, verificando che non vi siano contenuti occultati e nel caso procedendo ad analisi dei medesimi[3].

È ovvio che più il programma di analisi è moderno e aggiornato più sarà in grado di scovare file nascosti e di conseguenza maggiore sarà la resa in termini di risultato finale.

Qualora, invece, i file siano protetti da *password*, occorrerà procedere allo sblocco del loro contenuto mediante attacchi *brute force* volti all'individuazione della chiave che custodisce i dati[4].

In estrema sintesi e senza tecnicismi, l'attività di individuazione della *digital evidence* è suddivisibile in due

fasi: la prima è quella di acquisizione in copia forense della memoria del dispositivo, mentre la seconda prevede l'analisi della copia estratta, fase nella quale, più precisamente, vengono rintracciate e identificate le evidenze digitali stoccate in memoria che si sospettavano poter essere presenti sul dispositivo al momento del sequestro.

Per entrambe le fasi, in situazioni particolari, possono profilarsi problemi di sicurezza informatica. Durante tali momenti, ad esempio, delle criticità potrebbero insorgere qualora il dispositivo da acquisire e analizzare sia infetto da un virus informatico. Clonando la memoria inevitabilmente verrebbe clonato anche il programma malevolo, che per conseguenza si estenderebbe alla copia forense.

Ora, se l'infezione sul dispositivo originario fosse nota, il problema in realtà non si porrebbe. In tal caso, infatti, l'ostacolo potrebbe essere facilmente aggirato acquisendo più copie del dispositivo e quindi procedendo alla disinfezione del virus da una di esse, per poi confrontarla con le altre per valutare se l'operazione di eliminazione del *malware* abbia comportato la compromissione di dati oppure abbia mantenuto inalterate le informazioni[5].

Il problema emerge quando il virus informatico passa inosservato all'occhio dei *software* adoperati per le operazioni forensi. Si consideri sul punto che, al pari degli altri programmi informatici, anche gli strumenti adoperati per la *digital forensics* possono avere delle vulnerabilità nella sicurezza, soprattutto quando il sistema non viene regolarmente aggiornato. In linea teorica, pertanto, potrebbe capitare che un *malware* sfugga al controllo e continui a svolgere indisturbato il compito per il quale è stato progettato.

In particolare, esistono alcuni tipi di *malware* che una volta sottoposti all'azione dei programmi di analisi sono in grado di corromperne l'algoritmo e alterarne il funzionamento per

far commettere al *software* operazioni per le quali originariamente non era settato o che non era stato autorizzato a svolgere. È superfluo specificare che in simili evenienze l'attendibilità delle risultanze ottenute con l'analisi forense sarebbe del tutto assente.

Ad ogni modo, vulnerabilità di questo tipo non colpirebbero la genuinità del procedimento di formazione della copia forense, ma esclusivamente il successivo passaggio di analisi, compromettendo quindi non l'acquisizione in sé (consistente in una mera copiatura dei *byte* della memoria originale senza attività di elaborazione) ma solo i sistemi di analisi e in conseguenza l'analisi che ne scaturisce[6].

Un recente caso di cronaca, andato alla ribalta delle testate giornalistiche che si occupano di cybersicurezza, ha messo in chiaro come quanto appena descritto non sia solo un'ipotesi di scuola, bensì potrebbe realmente accadere, o meglio, sarebbe già accaduto. Il caso riguarda lo scambio di battute avutosi tra fine 2020 e prima metà del 2021 tra la nota app di messaggistica Signal e l'azienda israeliana produttrice di strumenti di informatica forense – tra le più affermate sul mercato – Cellebrite Ufed.

La disputa aveva origine allorché l'azienda israeliana comunicava pubblicamente di aver trovato il modo per violare le difese dell'applicazione di messaggistica – come noto tra le più sicure e tra le più improntate alla garanzia della privacy degli utenti – affermando di esserne persino riuscita decifrare i contenuti delle chat e i relativi allegati. Successivamente, sebbene l'azienda, sul presupposto delle polemiche che stavano emergendo, avesse tentato di ridimensionare la portata sensazionalistica della comunicazione originale, si scatenava ugualmente la reazione di Signal.

Per tutta risposta infatti quest'ultima, a mezzo di un articolo pubblicato pochi mesi dopo dal proprio amministratore

delegato[7], nello sminuire ulteriormente la notizia dell'hackeraggio[8] controbatteva insinuando di essere stata a sua volta in grado di individuare alcune vulnerabilità presenti sul *software* di analisi *Physical Analyzer*, sviluppato e distribuito sul mercato dalla società israeliana.

In pratica, secondo l'amministratore delegato di Signal, il *software* della Cellebrite dopo il lancio nel 2012 non sarebbe più stato implementato con i necessari aggiornamenti, sicché avrebbe presentato diverse falle nel proprio sistema di sicurezza. Sfruttando queste mancanze sarebbe stato possibile eseguire sul *software* dei codici capaci di modificare sia i report di Cellebrite relativi all'attacco sia quelli precedenti e futuri, creati a partire da dispositivi acquisiti in precedenza. Inoltre, sarebbe stato possibile attuare modifiche rilevanti nel contenuto analizzato: inserire o rimuovere parti testuali, messaggi di posta elettronica, immagini, contatti, file e qualunque tipo di dato, il tutto sfuggendo completamente ai controlli dei *checksum*. Nei casi peggiori, come riporta sempre Signal, un attacco simile avrebbe addirittura potuto causare la fuoriuscita dei dati presenti sul dispositivo analizzato, il tutto con ovvia ripercussione sull'attendibilità dell'analisi stessa[9].

Il caso appena esaminato rende evidente le maggiori criticità di *cybersecurity* che possono inficiare la funzionalità degli strumenti per le analisi forensi. Il rischio è che *malware* capaci di agire nei termini su visti possano presto divenire una realtà largamente diffusa.

Secondo gli esperti, tuttavia, si potrebbe ricorrere ad alcune contromisure. In particolare, per ovviare alle problematiche di file illeciti di questo genere una soluzione potrebbe essere quella di rivolgere lo sguardo agli strumenti di *machine learning;* ovvero a algoritmi che facendo ricorso a logiche matematiche e di elaborazioni computazionale sono in grado di apprendere informazioni direttamente dai dati che gli

vengono sottoposti, senza che abbiano ricevuto in precedenza delle istruzioni specifiche. Una volta "addestrati" questi algoritmi sono in grado di adattarsi a situazioni nuove e potenzialmente, in chiave predittiva, a riconoscere programmi che si comportano in maniera difforme dalla normalità, potendo quindi teoricamente scoprire file malevoli che si camuffano da altri programmi.

L'applicazione delle logiche del *machine learning* alla *digital forensics*[10], in fase di esame della copia forense, potrebbe quindi aiutare il programma di analisi a individuare possibili programmi malevoli e catalogarli come file sospetti.

Su un piano più tecnico gli algoritmi di *machine learning*, operando una verifica dei metadati dei programmi presenti sulla copia, sarebbero in grado di comprendere se un file possa essere potenzialmente dannoso mediante un confronto con i metadati di programmi già noti al sistema o dal medesimo già considerati sospetti[11].

Di certo l'applicazione degli algoritmi di *machine learning* non può costituire l'unica soluzione. Una buona strategia difensiva non può prescindere, ad esempio, dal costante aggiornamento del sistema e dalla applicazione delle altre comuni buone pratiche e accorgimenti che costituiscono i principi fondanti della sicurezza informatica.

Questo articolo è stato estratto dal white paper "**La Digital forensics nel processo penale**" disponibile in maniera libera e gratuita al seguente link: https://www.ictsecuritymagazine.com/pubblicazioni/digital-forensics-nel-processo-penale/

## Note

[1] Per un approfondimento delle diverse tipologie di *software* che vengono utilizzati nelle operazioni di informatica forense

e sul funzionamento degli stessi si rimanda a M. VITIELLO, "*Il laboratorio di informatica forense: i software, gli strumenti hardware, i costi*" consultabile sul sito https://www.agendadigitale.eu/documenti/il-laboratorio-di-informatica-forense-i-software-gli-strumenti-hardware-i-costi/#:~:text=Ad%20esempio%20Magnet%20Axiom%20%C3%A8,maggior%20numero%20di%20evidenze%20possibili.

[2] Si rammenta che per impedire che i dati da acquisire vengano corrotti dallo strumento di acquisizione medesimo è necessario che questo abbia la funzione di blocco di scrittura (*write blocking*).

[3] Per recuperare file cancellati oppure danneggiati vengono impiegati appositi strumenti di *file recovery* che servono proprio a ripristinare contenuti parziali.

[4] L'attacco di *brute force* «*consiste nel provare tutte le possibili combinazioni di lettere, caratteri speciali e numeri finché non individua la mescolanza giusta. Un'operazione che viene, ovviamente, eseguita da un software. Il tempo di riuscita dell'impresa dipende dalla velocità di calcolo del computer, nonché dalla complessità e la lunghezza della password (quanti e quali caratteri sono stati utilizzati)*». La definizione è tratta da R. RIJITANO, "*Brute force: cosa sono, come fare e prevenire gli attacchi a forza bruta*", consultabile sul sito https://www.cybersecurity360.it/nuove-minacce/brute-force-cosa-sono-gli-attacchi-a-forza-bruta-come-farli-e-prevenirli/.

[5] Ovviamente, in ogni caso, in sede processuale bisognerà capire se e in che modo il programma malevolo possa aver corrotto le informazioni sulla copia originale prima che venisse rilevato.

[6] Quanto finora riferito e la disamina che segue trae le mosse da P. DAL CHECCO, "*Signal ha hackerato Cellebrite, svelate*

*vulnerabilità nelle app di hacking telefonico: i risvolti*", in Cybersecurity360 consultabile sul sito https://www.cybersecurity360.it/nuove-minacce/signal-ha-hackerato-cellebrite-svelate-vulnerabilita-nelle-app-di-hacking-telefonico-i-risvolti/.

[7] L'articolo è consultabile sul sito Signal >> Blog >> Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective.

[8] Secondo quanto sostenuto da Signal, infatti, in realtà Cellebrite sarebbe riuscita semplicemente a capire dove si trovasse la chiave di cifratura con la quale i messaggi venivano localmente cifrati, cioè sul dispositivo analizzato, e non a forzare il meccanismo di cifratura delle chat dell'applicazione.

[9] Per un maggiore approfondimento si rimanda nuovamente a P. DAL CHECCO, op. cit., in *Cybersecurity360*.

[10] Si rimanda a N. BASSETTI, "*Machine learning per l'identificazione dei file sospetti: tecniche e sviluppi*", in Cybersecurity360, consultabile sul sito https://www.cybersecurity360.it/soluzioni-aziendali/machine-learning-per-lidentificazione-dei-file-sospetti-tecniche-e-sviluppi/.

[11] *Ibidem*.

Articolo a cura di **Francesco Lazzini**

Profilo Autore

Laureato in giurisprudenza con successivo conseguimento dei master in Scienze Forensi (Criminologia-Investigazione-Security-Intelligence) e in Informatica giuridica, nuove tecnologie e diritto dell'informatica. Attività di studio

postuniversitario focalizzata in materia di indagini con l’utilizzo del captatore informatico e digital forensics.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/digital-forensics-e-cyber-security-caso-cellebrite-ufed-vs-signal/