PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4779 di Mercoledì 23 settembre 2020

Criminologia informatica: quali novità?

I reati informatici spesso richiedono l'assistenza di specialisti del settore, in grado di operare come consulenti di ufficio consulenti tecnici di parte, per giungere alla ricostruzione degli aventi all'accertamento delle responsabilità.

Sempre più spesso le cronache ci danno notizia di violazioni di sistemi informatici, che possono portare a conseguenze significative, nei confronti del patrimonio dell'azienda coinvolta, nei confronti della sua immagine e nei confronti dei soggetti danneggiati da queste violazioni. Ecco perché è opportuno che i lettori siano aggiornati sulla modalità di reperimento di esperti del settore, dotati di credenziali accettabili.

Negli Stati Uniti questo problema è stato affrontato già da tempo, tant'è vero che l'istituto nazionale per la giustizia, ha creato un centro di eccellenza per la tecnologia criminologica (traduzione italiana dell'espressione inglese *forensic*). L'obiettivo di questo centro di eccellenza è quello di migliorare le competenze dei soggetti coinvolti, utilizzando tecniche estremamente avanzate, in grado di convincere il giudice e giurie della validità delle analisi e delle conclusioni degli esperti. Negli ultimi tempi, l'attenzione dei responsabili di questo centro di eccellenza si è concentrata in particolare sulle indagini criminologiche, afferenti alle violazioni di sistemi informativi, organizzando dei corsi di formazione a distanza, che stanno incontrando un successo straordinario. Chi scrive ha recentemente partecipato ad un corso di formazione sull'acquisizione e la valutazione dell'evidenza digitale, da utilizzare a supporto delle posizioni, sia dell'accusa, sia della difesa.

Ormai leggiamo tutti i giorni sui giornali che, quando si verificano frodi informatiche o violazioni dei dati, le forze dell'ordine provvedono alla asportazione dei computer reperiti presso i soggetti coinvolti, per condurre successive analisi.

Queste analisi devono permettere agli esperti di raggiungere delle conclusioni, che devono essere messe a disposizione dell'accusa e della difesa, per l'appropriato utilizzo in fase giudiziaria.

Oggi sono disponibili degli applicativi, alcuni gratuiti, altri a pagamento, che permettono di estrarre dati nel computer, offrendo ogni garanzia circa il fatto che tali dati non siano in alcun modo alterati o alterabili. Il corso di formazione ha illustrato i partecipanti i vari applicativi disponibili, elencandone pregi e difetti.

Un aspetto significativo, nella scelta dell'applicativo di estrazione dei dati, riguarda soprattutto la massa di dati da estrarre. Si tratta infatti di un aspetto assai importante, perché talvolta i dati da esaminare raggiungono volumi straordinariamente elevati, che non sempre possono essere correttamente gestiti da applicativi non specializzati.

Ecco i nomi di alcuni di questi applicativi, che dovrebbero essere già noti ai nostri lettori:
snort, *pcap*, *TcpDump*, *wireshark,* e *NetworkMiner.*

Il docente ha anche illustrato altri applicativi, questa volta a pagamento, che offrono tuttavia la possibilità di intervenire in modo assai più articolato sui dati estratti. Infine, si faccia attenzione al fatto che questi applicativi possono lavorare sia a posteriori, su archivi digitali già memorizzati, sia in tempo reale, su dati in corso di elaborazione.

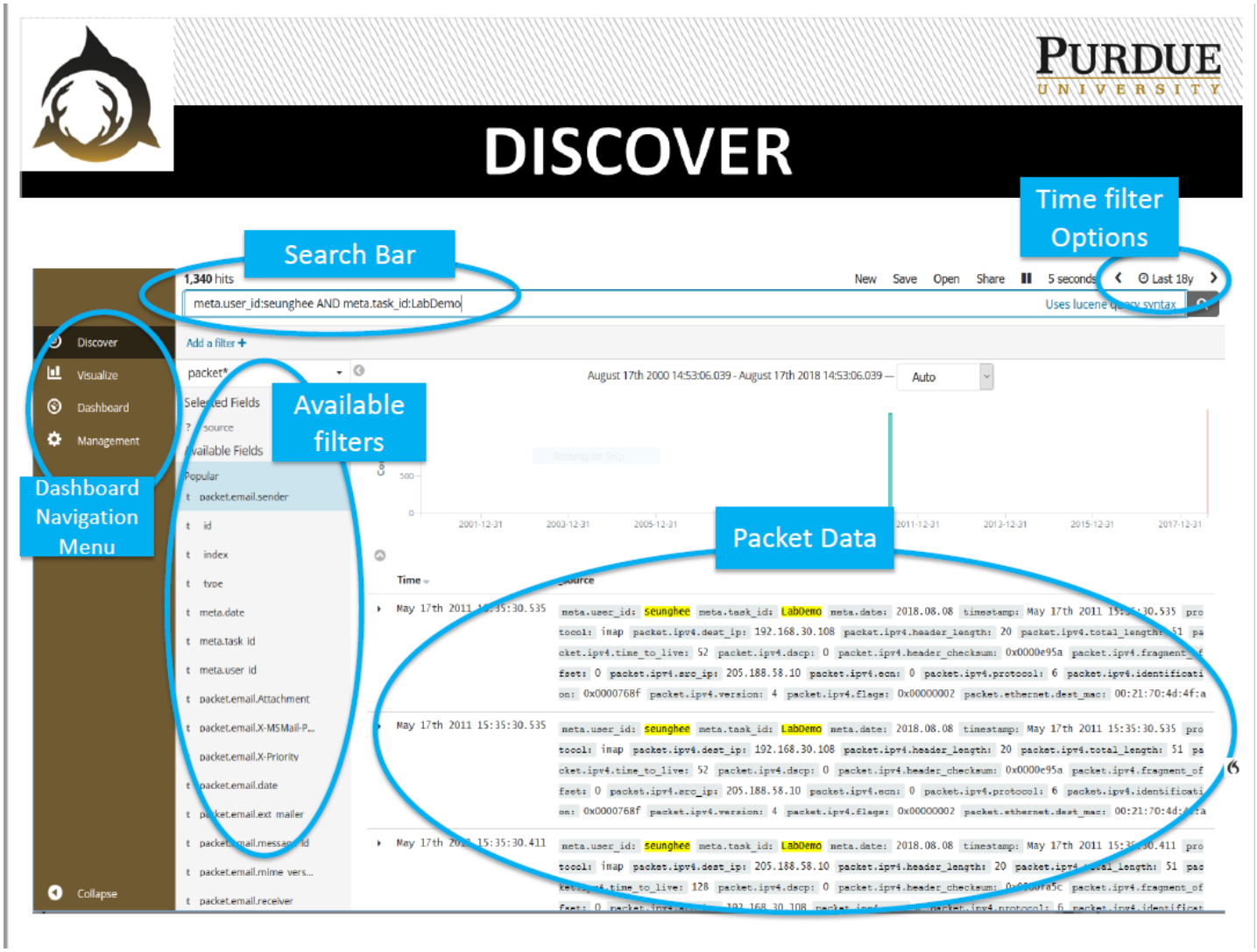
Un altro aspetto da prendere in considerazione è legato al numero di computer da esaminare, durante la consulenza tecnica. Oggi non è insolito il fatto che, quando la violazione coinvolge una grande azienda, siano migliaia i computer da analizzare, per individuare quello presso il quale la violazione ha avuto origine.

Con l'occasione, è bene ricordare come le indagini criminologiche informatiche si articolano in varie fasi:

- l'identificazione dei dati che devono essere raccolti, facendo attenzione al fatto che potrebbero essere raccolti file di vario tipo, come ad esempio file Word, PDF, JPEG e simili,
- la raccolta di questi dati,
- la sicurezza della catena di custodia di questi dati,
- l'analisi dei dati raccolti,
- l'elaborazione del rapporto, conseguente all'analisi dei dati.

Se questi passi non vengono attuati con tutte le appropriate garanzie, le valutazioni finali dell'esperto potrebbero essere contestate da controparti interessate.

Per finire, offro ai lettori un esempio di come un applicativo può presentare i dati raccolti, per offrire una agevole interpretazione del significato dei dati e consentire quindi agli esperti di giungere a conclusioni documentate e pertanto credibili.



Adalberto Biasiotti

www.puntosicuro.it