LA SICUREZZA DELLE INFORMAZIONI AL TEMPO DI WIKILEAKS

DAL "NEED-TO-KNOW" AL "NEED-TO-SHARE" E RITORNO

Stefano Ramacciotti

"Il progresso tecnologico è come un'ascia nelle mani di un criminale patologico."
(Albert Einstein)

L'antefatto

Negli ultimi tempi sui media è stato tutto un gran parlare di WikiLeaks, di ciò che è stato perso (sia in termini di informazioni che in termini di sicurezza), di come dovrà cambiare la diplomazia, e di molto altro. Però, poco si è detto di qual è stata la vera origine del problema, di come sia potuto accadere in America di certo uno dei Paesi più all'avanguardia nel campo della sicurezza informatica, e di quali misure attuare perché ciò che è accaduto non si ripeta più.

WikiLeaks (http://it.wikipedia.org/wiki/File:Wikileaks_logo.svg)

Partiamo, allora, da cosa è successo, ovviamente secondo quanto è stato reso di pubblico dominio. Un soldato ventitreenne, più esattamente il *Private First Class* (Caporal Maggiore) Bradley Manning[1], non si sa ancora bene per quale motivo ma, stando a quanto si è appreso, forse perché si sentiva frustrato o deluso[2] sul lavoro, si è reso colpevole della più massiccia rivelazione di informazioni classificate della storia di cui si abbia mai avuto notizia. Il militare in questione era assegnato in Iraq alla 2nd *Brigade Combat Team* della *10th Mountain Division* di stanza alla *Contingency Operating Station* ad Hammer, 40 miglia ad Est di Bagdad, in Iraq. In qualità di analista di Intelligence dell'U.S. Army aveva certamente accesso a numerose informazioni classificate attraverso la rete SIPRNet *(Secret Internet Protocol Router Network)* utilizzata dal Dipartimento della Difesa USA e dal Dipartimento di Stato e, probabilmente, anche attraverso la JWICS *(Joint Worldwide Intelligence Communications System)*. In virtù del proprio compito, secondo quanto finora trapelato, è stato facile per lui appropriarsi di numerosi dati. Servendosi di un CD riscrivibile sul quale aveva salvato della musica, per la cronaca *"Telephone"* di Lady Gaga, ha cancellato le canzoni e copiato sul CD le informazioni classificate alle quali aveva avuto accesso. Niente di più semplice.
Un recente articolo[3], tratto dalla versione online di Wired, riporta che l'accusato avrebbe utilizzato un software di data-mining[4], per ben due volte. Questo tipo di software non è di facile utilizzo; soprattutto la messa a punto del sistema richiede competenze tali che la rivista ipotizza che il Manning possa aver avuto bisogno di un supporto esterno e comunque dimostra la premeditazione e ne aggrava la posizione di indagato.

PFC Bradley Manning (http://www.haisentito.it/img/bradley-manning.jpg)

1 Sonia Verma, *Prime suspect felt "regularly ignored"*, The Globe and Mail, Canada, December 7, 2010 *(data on Manning)*.
2 Wired.com, *"I Can't Believe What I'm Confessing to You': The Wikileaks Chats"*, http://www.wired.com/threatlevel/2010/06/wikileaks-chat.
3 Kim Zetter, *Army: Manning Snuck 'Data-Mining' Software Onto Secret Network*, http://www.wired.com/threatlevel/2011/04/manning-data-mining/, del 4 aprile 2011.
4 Data mining: sistema che permette l'estrazione di informazione utile da insiemi di dati.

Le informazioni trafugate (circa 250.000 messaggi di cui 15.000 segreti) sono poi arrivate al noto Julian Assange, giornalista, sviluppatore di software e attivista Internet *(hacktivist)* australiano, che, per adesso, ha provveduto alla sola pubblicazione di parte del materiale. In Internet sono reperibili i rimanenti documenti in formato cifrato (file "insurance.aes256"), per i quali è stata minacciata la rivelazione della password di accesso nel caso che vi fosse un accanimento delle Autorità nei confronti del creatore di WikiLeaks.

Julian Assange
(http://en.wikipedia.org/wiki/File:Julian_Assange_(Norway,_March_2010).jpg)

Non è ancora stata chiarita la posizione di un altro *hacker* di nome Adrian Lamo, che ha denunciato la fuga di notizie ad opera di Manning ma che in passato ha anche supportato il sito di WikiLeaks. Assange non ha finora confermato niente e anzi ha avvalorato il sospetto che altre persone potrebbero avere partecipato all'operazione di far uscire le informazioni dalle sedi previste.
La domanda sorge spontanea, cosa sarà andato storto? Dove sarà stato l'errore?
Nel fare questo però teniamo sempre ben presente che, per quante misure si possano adottare, il rischio non è quasi mai completamente eliminabile, o per dirla con il Prof. Eugene Spafford della Purdue University:
"L'unico sistema realmente sicuro è un sistema spento, affogato in un blocco di cemento, sigillato in una stanza dalle pareti schermate col piombo e protetto da guardie armate. E anche in questo caso ho i miei dubbi che possa essere sicuro."

Questione tecnica o gestionale?

In un mondo dove la pervasività dei sistemi informatici ha raggiunto livelli fino a poco tempo fa impensabili è inevitabile che la gran parte delle informazioni sia trattata con sistemi automatizzati. Pensiamo a una classica azienda. La maggior parte delle informazioni saranno contenute in DataBase o altri sistemi informatici che dovranno essere protetti da chi si occupa di Sicurezza ICT *(Information and Communication Technology)*. La gestione della sicurezza della totalità delle informazioni sarà ovviamente compito dell'area della Sicurezza delle informazioni (INFOSEC) con cui l'area precedente dovrà essere in strettissimo coordinamento, anche perché ne è parte integrante. Il tutto sarà supervisionato dall'area relativa alla sicurezza dell'intera Azienda o organizzazione.
Purtroppo, ancora oggi, c'è chi considera l'ambito del "sistema informativo" (che gestisce le informazioni tramite processi organizzativi gestiti da risorse umane e facendo uso di risorse materiali) svincolato da quello del "sistema informatico" (che è la parte del sistema informativo che utilizza le infrastrutture informatiche), o quanto meno li considera mondi diversi.
In realtà sono uno il sottoinsieme dell'altro e, così, si può dire che le misure di sicurezza da adottare nel sistema informatico, nel quale vi è una preponderanza di quelle a connotazione tecnica, siano solo un sottoinsieme delle misure da adottare per proteggere[5] l'intero sistema informativo.

[5] Occorre precisare che il termine "proteggere" assume qui un chiaro significato, e cioè che siano preservate la "riservatezza", l'"integrità" e la "disponibilità" (altrimenti sintetizzato in CIA dall'Inglese *Confidentiality, Integrity and Availability*) delle informazioni.

Un atteggiamento ancora più nefasto è quello di chi si ostina a confondere una parte per il tutto. Questi sono coloro che quando sentono parlare di furti di informazioni avvenuti con i computer vedono il tutto solo come un problema tecnico. Lo dimostra il fatto che qualcuno, sentendo parlare di dati trafugati e di computer, pensando a Assange e Lamo, al grido di manzoniana memoria: «l'untore, dagli! dagli! dagli all'untore!»[6] ha gridato subito all'*hacker*, croce e delizia del mondo moderno.

Ciò è vero, Assange stesso e i suoi collaboratori sono dei buoni *hacker*, lo hanno dimostrato. Sì è trattato certamente di un *leakage* (traducibile con perdita, fuoriuscita) di dati da un sistema di computer, ma ricondurre ciò che è accaduto a una semplice azione di *hacker* è riduttivo e ha un effetto deleterio, perché si rischia di vedere un solo aspetto della questione, quello tecnico, e di perdere di vista il vero problema che è più generale e riguarda la sicurezza delle informazioni nel loro insieme.

Ma, è certo che, affrontando la problematica solo da questo punto di vista si finisca per vedere solo una parte del problema, commettendo un grave errore.

Soprattutto nel nostro Paese, ottavo nel G8 ma molto più indietro nell'uso delle nuove tecnologie (*smart-phone* a parte), dove i termini sicurezza delle informazioni e sicurezza informatica[7] sono considerati, a torto o a ragione, un argomento ostico e per pochi specialisti.

Allora, quando c'è da trattare un problema in questo ambito ci si rivolge spesso a colui che riteniamo essere l'esperto della situazione (che spesso è solo un informatico con competenze quasi nulle, o molto limitate, nel campo della sicurezza) per avere suggerimenti, pensando che siano solo argomenti tecnici, ma non è così. Oltre che essersi, probabilmente, rivolti alla persona sbagliata, si commette un ulteriore errore perché un tecnico puro, per indole, è portato a pensare alle sole questioni tecniche, sorvolando ad esempio su ciò che è spesso più importante, ma meno stimolante per lui, cioè la parte procedurale, in gran parte trattata nella sicurezza del sistema informativo.

Della sicurezza del sistema informativo si occupa

[6] Netman, *Dalli [Sic!] all'untore!*, http://www.datamanager.it/news/sicurezza/dalli-all-untore, Newsletter del 6 dicembre 2010.

[7] Sicurezza di una rete o di un semplice computer, la cosiddetta *"computer security"*, o ICT Security o più semplicemente "sicurezza informatica" (nel seguito usati, anche se non propriamente, come sinonimi) si riferisce, perciò, al complesso delle misure di sicurezza, siano esse tecniche che organizzative che procedurali, poste in essere per proteggere il sistema informatico e le informazioni che questo tratta.

l'*Information Security*, abbreviata INFOSEC[8], anch'essa basata sui tre requisiti di sicurezza CIA (vedi nota 5) che rappresenta un concetto più generale che ha a che fare con la gestione *(management)* delle informazioni, la cui responsabilità risiede direttamente nel vertice di ogni organizzazione.

Facciamo un passo indietro e affrontiamo, per ora, la questione dal punto di vista squisitamente tecnico partendo dalla protezione classica per gli aspetti relativi alla riservatezza che è quella crittografica.

È evidente che, quello di WikiLeaks non è stato un problema legato alla crittografia. A parte l'accuratezza con la quale sono oggi verificati i sistemi destinati a offrire una protezione crittografica, le informazioni, nella postazione dell'utente autorizzata alla trattazione delle stesse, erano probabilmente "in chiaro".

Sicuramente erano previste anche altre contromisure tecniche che, o non sono state implementate o non hanno avuto effetto. Infatti, è lecito supporre che qualche misura tecnica volta ad assicurare la protezione della informazione dovesse essere stata posta in essere (come ad esempio il masterizzatore e le porte USB disabilitate, ecc.). È probabile però che se sulla postazione vi era un masterizzatore l'operatore della postazione fosse autorizzato ad utilizzarlo, per cui possono probabilmente essere escluse anche queste cause tecniche alla base della fuga di notizie.

È improbabile anche che sia stato un problema di scarsa conoscenza della normativa legale da parte dell'operatore. Infatti, considerando quanto sono scrupolosi gli statunitensi nella preparazione del proprio personale, è anche questo da escludere.

L'operatore doveva essere a conoscenza a cosa sarebbe andato incontro rivelando informazioni coperte dal segreto (si parla di un massimo di pena di 52 anni di reclusione e non di pena di morte come qualcuno ipotizza).

Allora qual è stata la vera causa della fuga di notizie?

È molto probabile che la ragione risieda semplicemente nel non avere rigorosamente seguito le procedure di controllo che era opportuno fossero applicate e che probabilmente in qualche manuale erano descritte. Cioè si è molto probabilmente trattato di un problema più generale legato all'*Information Security* che non alla sola *Computer Security*.

In realtà, oggi, è bene considerare il problema sempre nella sua interezza, e non fermarsi solo agli aspetti tecnici, al fine di ridurre i possibili problemi legati alle vulnerabilità intrinseche del sistema. Perché un sistema informatico non lo si protegge solo con la tecnica ma occorrono anche le procedure e ancor prima persone preparate e consapevoli che le utilizzano e le impongono correttamente.

Allora, se qualcuno doveva pur conoscere la procedure, come è lecito supporre, e c'erano anche persone sufficientemente preparate per farle rispettare, perché c'è stata la fuga di informazioni?

Una nuova malattia: la "sindrome di Fort Apache"

Mentre la *"maggior parte delle aziende di oggi ritiene che tutte e sole le minacce alla propria incolumità – specie se legate alla sfera delle tecnologie – vengano dal proprio esterno"* [9], è ormai provato che "oltre l'ottanta per cento degli incidenti di sicurezza che avvengono nelle aziende ha origine all'interno delle organizzazioni stesse". La situazione degli ambiti dove vengono trattate informazioni classificate è un po' diversa da quella di altri ambiti, come quello aziendale, perché il personale è periodicamente "passato

[8] Il concetto, usuale di INFOSEC è un po' diverso da quello della normativa di sicurezza italiana (DPCM 3/2/2006) che considera l'INFOSEC come l'unione dei due ambiti di *COMPUter SECurity, COMPUSEC*, e *COMmunication SECurity, COMSEC*.

[9] Giustozzi C., *La sindrome di Fort Apache. La sicurezza delle informazioni nella società postindustriale*, Trento, Ed. M&A, 2007, pagg. 15-16

al setaccio" con più approfondite attività di *screening* volte a rivelarne eventuali vulnerabilità ai fini del rilascio e mantenimento della *security clearance* (equivalente all'italiano NOS, nulla osta di sicurezza). Non è disponibile pubblicamente l'elenco dei criteri presi a riferimento dagli U.S.A. per il rilascio della security clearance, ma su Internet si trovano documenti[10] che appaiono verosimili, per essere usati come riferimento.

Se quanto sopra risponde al vero, sembra evidente che anche negli U.S.A. siano adottati criteri simili a quanto riportato nell'art. 22 del D.P.C.M 3 febbraio 2006 (Norme unificate per la protezione e la tutela delle informazioni classificate) in base al quale negare o revocare il NOS. È, però, altresì evidente che l'applicazione di tali verifiche, almeno in questo caso, non è stata sufficiente.

Ma se il Manning era stato attentamente vagliato, come è lecito supporre essendo, oltre a un militare, un militare impegnato nel campo dell'*intelligence*, di nuovo, perché è accaduta la fuga di notizie?

Vi sono almeno tre motivi riconducibili uno alla persona e due all'organizzazione:

1. minore percezione del crimine nel computer crime (problema dell'individuo tipico nelle situazioni di crimine "tecnomediato");
2. vaglio della persona non aggiornato (problema dell'organizzazione);
3. sindrome di Fort Apache (problema dell'organizzazione).

Come si può vedere non sono certo motivi "tecnici".

Per il primo motivo occorre notare che nel caso di computer le dinamiche criminali[11] sono alterate dalla bassa percezione che l'individuo ha della situazione intesa come: 1) gravità del comportamento; 2) conoscenza delle leggi in materia; 3) stima dei rischi di essere scoperto, denunciato e catturato; 4) percezione del danno inferto alla vittima e 4) timore della sanzione sociale e legale.

Basta pensare a quanti "scaricano" tranquillamente musica e film da Internet e che non sarebbero mai capaci di rubare un CD da un negozio di musica, quando la differenza tra i due atti consiste solo in un supporto di plastica da pochi centesimi di euro.

Per il secondo motivo le considerazioni sono diverse. Quanto accennato sopra unito a insoddisfazione riguardo al proprio lavoro, come: volontà di vendicarsi del datore di lavoro o dei superiori gerarchici, paga ritenuta inadeguata rispetto alle responsabilità, sensazione di non essere stimato dai colleghi e disturbi della personalità non individuati all'atto dell'assunzione e delle successive verifiche, possono rappresentare una bomba ad orologeria pronta ad esplodere in qualsiasi momento.

Il rischio, poi, si fa maggiore se la persona è coinvolta in una situazione particolarmente stressante, come probabilmente è capitato al Manning durante la sua missione in Iraq, stando a quanto trascritto nelle sessioni di *chat* occorse tra lui e Lamo[12]. Ergo, il controllo in situazioni limite, dove il personale è più stressato, anziché essere più superficiale, dovrebbe essere intensificato.

E da questa considerazione si passa al terzo motivo, che è, ancora più probabilmente, la vera causa della fuga di informazioni. È individuabile nella cosiddetta *sindrome di Fort Apache*, che non è altro che quell'atteggiamento secondo il quale si pensa che i "cattivi" stiano tutti fuori, e dentro il forte ci siano solo i buoni. Purtroppo, nonostante che le fughe di notizie siano quasi esclusivamente appannaggio degli *insider*, non si è forse posta ancora troppa attenzione all'argomento.

Se alla conoscenza dell'individuo e la consapevolezza che sia stato attentamente controllato si aggiunge la maggiore difficoltà nell'utilizzare

[10] http://usmilitary.about.com/od/theorderlyroom/blsecmenu.htm.
[11] Strano M. [e al.], *Inside attack. Tecniche di intervento e strategie di prevenzione*, Roma, Nuovo Studio Tecna, 2005, pagg. 45-50.
[12] Wired.com, *"I Can't Believe What I'm Confessing to You': The Wikileaks Chats"*, http://www.wired.com/threatlevel/2010/06/wikileaks-chat.

i controlli tecnici (è innegabile che sia più semplice controllare uno registro di apertura e chiusura di una porta che non un file di *log*[13] in cui i vari dati devono essere correlati fra loro per comprendere cosa è avvenuto) è comprensibile che il controllore si "rilassi" e che la fuga delle informazioni divenga possibile.

E questo è quanto sembra sia avvenuto nel caso del PFC Manning, in quanto componente dell'*intelligence* e pertanto persona ritenuta particolarmente attendibile perché aveva superato indenne numerosi controlli di sicurezza, e nei confronti del quale i previsti controlli potessero essere relativamente blandi o che non fosse proprio necessario applicare quelli dovuti. Sembra cioè che chi doveva controllare il comportamento del Private Manning fosse "affetto" dalla citata sindrome di Fort Apache.

Se questo atteggiamento era già errato in passato, lo è ancora di più dopo l'11 settembre (o il *nine eleven*, 9/11, come viene chiamato oltre Atlantico).

Per evitare, infatti, che una mancata correlazione delle informazioni disponibili permettesse un nuovo 11 settembre a causa di una compartimentazione troppo restrittiva dei dati, la politica di gestione delle informazioni U.S.A. si è "evoluta" dal classico *need-to-know* al nuovo *need-to-share* o meglio al *responsability-to-share*. Cioè prima l'informazione poteva essere comunicata solo a chi ne avesse la effettiva necessità (in pratica vagliando le richieste di accesso), dopo l'11/9 l'informazione acquisita deve essere condivisa con chi ne potrebbe avere bisogno, con un passaggio da un'ottica *pull* ad una *push*.

È evidente che un tale cambiamento doveva generare una nuova analisi dei rischi che non poteva non richiedere un ulteriore supplemento di misure di sicurezza volte a limitare la possibile fuga di informazioni sensibili.

Purtroppo dette misure non sembra che siano state perfettamente applicate e una eccessiva fiducia nel proprio personale abbia fatto il resto.

Conclusioni

Vediamo cosa avrebbe dovuto almeno fare colui che aveva la responsabilità della sicurezza nel caso Manning, se non fosse stato affetto, anche lui come molti, dalla Sindrome di Fort Apache. Queste sono le contromisure che avrebbero permesso di contenere le perdite, e cioè:

- adeguato trattamento del rischio con particolare riguardo al suo continuo aggiornamento, in modo da tener conto dei cambiamenti di situazione;
- indottrinamento più capillare sia ai "controllori" e sia agli utenti, evidenziando come situazioni più stressanti possano comportare maggiori rischi;
- intensificazione dei controlli sulle persone (in particolare sugli *insider*);
- policy più restrittive in merito alla gestione degli account di accesso al sistema informatico (creazione *account*, revisione periodica, registrazione di ogni più piccolo cambiamento nel sistema, ecc.) con controlli più rigorosi dei profili di accesso ai sistemi critici e per i quali sia effettuato un controllo capillare sull'applicazione degli stessi;
- maggiori controlli fisici all'ingresso dell'area classificata, per evitare l'uso di CD riscrivibili o iPod (per evitare la pericolosa tecnica chiamata *Pod slurping* [14]) o altri sistemi di memorizzazione di massa;
- più granulari procedure fisiche all'uscita dall'area controllata, con verifica del materiale portato all'esterno (la sicurezza nazionale non può scendere a compromessi con la privacy o le leggi relative alle perquisizioni);

[13] I file di log sono quei file in cui sono memorizzate, in ordine cronologico, le principali operazioni che avvengono all'interno di un computer, cioè sono i file contenenti la "storia" di ciò che è avvenuto su un computer. Esistono log di sistema, di sicurezza, relativi alle applicazioni, ai database, ecc.. Per verificare un tentativo di accesso non autorizzato occorre spesso correlare tra loro diversi eventi, azione difficoltosa in assenza di appositi software e/o conoscenze adeguate.

[14] *"Pod slurping"* che consiste nel copiare GB di dati semplicemente connettendo un iPod opportunamente preparato ad una porta USB, magari con la semplice scusa di ricaricarlo.

- classificazione dei dati in base a criteri ben definiti, con compartimentazione adeguata degli stessi e più granulari permessi logici di accesso (con misure tecnico/organizzative per "qualificare" opportunamente le informazioni e restringere il campo solo a chi in possesso del *need-to-know*) e di come i file possono essere trasferiti. In casi come questo potrebbe essere opportuno applicare anche la cosiddetta *separation of duties*, concettualmente simile alla *two-men-rule* utilizzata per il lancio dei missili balistici, in modo da non permettere ad esempio il back-up di un sistema ad una sola persona, incrementando e imponendo maggiori controlli anche sul personale amministratore;
- procedure logiche[15] per evitare che si potessero copiare ingenti quantità di informazioni passando completamente inosservati (argomento sul quale gli statunitensi stanno alacremente lavorando per la realizzazione di opportuni sistemi atti a contenere le perdite[16]). Ciò implica software per consentire di monitorare l'utilizzo di dispositivi esterni e un attento lavoro di controllo, in via continuativa per assicurare la prevenzione, e analisi, *post mortem* (come dicono gli esperti in *forensic analysis*), dei *log* del sistema al fine di individuare anomalie significative relative ad azioni di *file transfer* o *download*;
- non concedere la possibilità di installare software non autorizzato (compresa la disabilitazione dell'avvio automatico da CD/DVD o chiavetta USB sui sistemi operativi che hanno questa modalità);
- software per consentire di monitorare le attività on-line (come il blocco di accesso a determinati siti), le e-mail e l'accesso remoto, così come il monitoraggio ed il tracciamento di documenti sensibili, il *key-logging* delle applicazioni aperte, ecc.. Ciò implica il divieto di uso di crittografia forte su sistemi connessi a Internet. La crittografia forte rappresenta infatti sia la soluzione che il problema. La soluzione perché permette di proteggere il contenuto informativo, un problema perché è il sistema che permette di celare le informazioni ad un sistema di filtraggio in grado di bloccare la fuoriuscita di informazioni sensibili in base a determinate parole chiave;
- un piano di risposta agli incidenti adeguato.

Ciò sempre se i presupposti, cioè le informazioni pubblicamente disponibili, siano vere, elemento che non è possibile appurare con certezza.

Tutto ciò che è stato riportato non vuole essere nel modo più assoluto una critica a chi più di tutti, cioè agli "americani", ha contribuito allo sviluppo della sicurezza informatica e informativa. Quanto è successo sarebbe potuto capitare a qualsiasi altra organizzazione. Bisogna però sfruttare ciò che è accaduto affinché si possa "gestire il rischio", che non è quasi mai eliminabile completamente ma che deve essere almeno ridotto al minimo, grazie all'applicazione delle cosiddette *best practices*, molto citate ma sempre troppo poco applicate.

Occorre acquisire una nuova consapevolezza dell'importanza della materia sicurezza informatica e delle informazioni. È nostro dovere, perché da ciò dipende la sicurezza di tutti.

In tale ambito anche la Difesa italiana ha aggiornato la propria politica di sicurezza promuovendo una serie di misure procedurali e tecniche per fronteggiare più efficacemente le minacce rappresentate.

Noi abbiamo avuto la nostra "notte di Taranto" e gli Americani, nel '41, cioè un anno dopo, la loro Perl Harbour; ora nonostante un approccio pragmatico ed efficiente gli Americani hanno avuto la loro Perl Harbour virtuale, WikiLeaks, ... noi non vogliamo certo rischiare un'altra notte di Taranto, questa volta virtuale! ■

[15] Noah Shachtman, *Military Bans Disks, Threatens Courts-Martial to Stop New Leaks*, <http://www.wired.com>, December 9, 2010 *(immediately cease use of removable media on all systems, servers, and stand alone machines residing on SIPRNET).*

[16] Spencer Ackerman, *Darpa's Star Hacker Looks to WikiLeak-Proof Pentagon,* <http://www.wired.com>, August 31, 2010 *(Darpa's new project is called CINDER, for Cyber Insider Threat).*