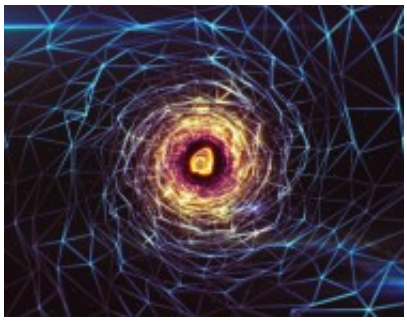
Cyber security le nuove sfide

Date : 9 febbraio 2016



> Sempre più spesso, sui principali giornali, leggiamo notizie di attacchi informatici più o meno complessi alle più svariate tipologie di aziende, istituzioni e ultimamente anche a soluzioni e/o prodotti.

Nel corso del 2013 si è notata una vera e propria escalation di reati e frodi, realizzati tramite la compromissione delle reti e dei collegamenti ad internet. Pensiamo a quanto successo in questi ultimi due mesi e prendiamo ad esempio queste due tipologie di attacchi: 30 novembre, l'attacco al sito della regione Lombardia; 4 ottobre, il furto ad adobe di codici e dati di 3 milioni di carte di credito.

L'attacco al sito della regione ha sicuramente una valenza istituzionale ed è facilmente immaginabile quali possano essere le cause che hanno spinto questi soggetti ad effettuare un modo non comune di protesta mediante un attacco informatico. Maggiore preoccupazione pone, invece, quanto successo ad Adobe. La causa principale, dell'attacco è sicuramente quella economica; sappiamo tutti che, oramai, i numeri delle carte di credito, gli elenchi di clienti e/o fornitori hanno in certi ambienti un notevole mercato sempre più fiorente. Come si può ben capire, i tradizionali sistemi di attacco informatico sono sì sempre attuali e remunerativi, ma le nuove sfide sposteranno sicuramente i target di attacco. Si passerà da attacchi più o meno generalizzati o volti a ledere l'immagine dell'attaccato ad attacchi che, con metodi nuovi e sempre maggiormente mirati, avranno come solo scopo venale quello di "fare soldi". Senza dimenticare i motivi politici ed ideologici più o meno legittimi, nella maggior parte dei casi, il vero motivo per il quale gli hacker hanno interesse è, però, quello rivolto al business.

Quanto detto è certamente causa di preoccupazione per le aziende e istituzioni, ma fa parte dei pericoli che si possono definire"conosciuti" e di fronte ad essi sappiamo come provare a difenderci. Purtroppo si stanno affacciando nuove tipologie di attacchi, che definirei maggiormente "pericoli".

Cercherò in queste poche righe di illustrare quelle che potrebbero essere le nuove sfide o tipologie di attacchi informatici non più combattute con armi tradizionali. Grazie alla sempre maggiore connessione con internet, anche i nostri stessi elettrodomestici potrebbero diventare dei veri e propri pericoli nel mondo informatico.

Proviamo, quindi, a disegnare il nuovo orizzonte operativo dei pirati informatici, effettuando un viaggio tra le loro possibili nuove minacce. Considerando che “ogni rete ha una falla, ogni network è vulnerabile”, dovremmo iniziare a prendere in considerazione che anche gli elettrodomestici, i mezzi di trasporto (Bus, Treni e aerei), le apparecchiature sanitarie, le TV, etc., diventeranno i nuovi sistemi da attaccare. Ecco il motivo per il quale tutte le maggiori società che si occupano di cyber crime stanno cercando di capire e scoprire i prossimi obbiettivi attraverso cui il crimine informatico intende accrescere un business stimato in miliardi di euro l’anno (più di quanto rendano i traffici di sostanze stupefacenti!).

Non è una novità che già oggi sia possibile accedere ai nostri nuovi pacemaker, i quali utilizzano sistemi di comunicazione wireless per trasferire al centro di controllo dell’ospedale o del medico i dati dell’apparato e, qualora si rendesse necessario, questi potrebbero essere modificati a seconda delle condizioni del paziente. Immaginiamo cosa potrebbe accadere, se dovesse esserci un effettivo interesse da parte di criminali a forzare per via telematica tali apparati e procedere alla modifica indiscriminata dei parametri di configurazione. Sicuramente il risultato sarebbe quello di creare seri danni alle persone portatrici di tali sistemi ed in alcuni casi di causarne anche la morte. Oppure pensiamo ai nostri nuovi televisori, i tanto reclamizzati smart TV, che una volta collegati alla rete diventano dei veri e propri computer, con cui poter effettuare una notevole quantità di operazioni. Immaginate cosa accadrebbe se un hacker riuscisse a penetrare in tali sistemi e quanti danni potrebbe causare ad essi. Potrebbe utilizzare la nostra rete come veicolo per attacchi informatici o, peggio ancora, potrebbe utilizzarli per verificare la nostra presenza nelle case per eventuali furti. Pensiamo alla nuova generazione dei nostri elettrodomestici, anche loro sempre più connessi alla rete: cosa potrebbe accadere se un ragazzino, per gioco (visto che i tools di attacco si trovano facilmente in internet), forzasse il loro sistema e iniziasse a inviare richieste di acquisto a vari negozi? Non dimentichiamo poi l’utilizzo degli smartphone che sono dei veri e propri cavalli di troia per entrare nei nostri sistemi, capire le nostre informazioni e modificare il nostro stile di vita. Quanti di noi hanno un antivirus installato su questi apparecchi o effettuano il backup almeno della rubrica?

Scenari simili non risparmiano neanche la nautica. Infatti sono state riscontrate vulnerabilità nei sistemi di comunicazione delle imbarcazioni, che, se ben sfruttate, potrebbero consentire di lanciare finti segnali di soccorso o, peggio, spingere un’imbarcazione fuori rotta. Improbabile?

Questa estate il professore Todd Humphreys, esperto di tecnologia satellitare di navigazione e di sicurezza, ha dimostrato che una vulnerabilità Gps potrebbe consentire agli hacker e terroristi di dirottare navi, droni e aerei di linea commerciali. Il professore con un apparato economico composto di una piccola antenna, un sistema elettronico Gps “spoofer” costruito con soli 3.000 dollari (2.260 Euro), e un computer portatile, è stato in grado di prendere il controllo totale del sofisticato sistema di navigazione di un super-yacht di 64 metri nel Mar Mediterraneo ed ha spiegato come, con il suo team, abbia sfruttato tale debolezza per il controllo della nave: «Sono stati iniettati alcuni nostri segnali di spoofing nelle antenne Gps della nave in grado di controllare il sistema di navigazione del natante con i loro segnali. Teniamo presente che sia il comandante che l’equipaggio non hanno notato nulla di anomalo nella strumentazione».

Pensiamo un attimo a cosa potrebbe accadere se non fosse un gioco o, come in questo caso, soltanto un test, considerando che circa il 90 per cento delle merci del mondo viaggia attraverso

i mari… Il dirottamento con relativa collisione di una nave da crociera o di una petroliera in termini di perdita di vite umane e di impatto ambientale porterebbe a conseguenze devastanti. I casi come quello della Costa Concordia e dell'Exxon Valdez sono stati l'esempio più clamoroso dell'effetto di incidenti marittimi. L'analisi non può essere limitata al solo ambiente marittimo, ma lo stesso tipo di attacco può essere condotto su tutte le tecnologie che utilizzano il Gps.

Tutto ciò potrebbe sembrare fantascienza, ma non è così. La sempre maggiore interconnessione dei nostri sistemi e apparati, se non ben gestita a livello di sicurezza, potrà causare seri danni a tutta l'economia. Teniamo sempre presente che la maggior parte degli attacchi informatici hanno un solo scopo: "il guadagno". Violare un pc, sottrarre dati, mettere ko interi sistemi o siti web sono di fatto imprese superate. Gli hacker, entro i prossimi tre anni, saranno in grado di spiare le case utilizzando le telecamere presenti su televisori, consolle, baby monitor, tablet e smartphone. Sarà loro possibile spegnere un frigo, accendere un condizionatore, sabotare macchine e tanto altro attraverso qualsiasi oggetto connesso alla rete.

L'unica possibilità che abbiamo è quella di cercare di mitigare (mitigare non eliminare!) gli effetti dei vari attacchi a cui saremo soggetti, mediante l'adozione di opportuni comportamenti e policy di sicurezza sia in azienda che nelle nostre stesse case, al fine di ridurre in modo sensibile l'esposizione al rischio di attacco, che avrà come unico scopo primario quello di trarne profitto economico.

La risposta che possiamo darci è che per molti di noi la percezione della sicurezza delle informazioni ha nella nostra scala di priorità il valore più basso, per non dire nullo.

A cura di **Bruno Carbone**, ICT Security & Privacy Expert

Articolo pubblicato sulla rivista ICT Security – Gennaio/Febbraio 2014