Intervista a SBS Radio – Australia



I microfoni di SBS Radio, l’emittente “Poliglotta” australian, intervistano Luca Poma, autore – per Franco Angeli editore – del libro “Il sex appeal dei corpi digitali”
Ascolta l’audio:
http://corpidigitali.it/wp-content/uploads/2015/08/italian_160626_514647.mp3

Nota sul copyright e sulla

protezione brevettuale

Nota sul copyright e sulla protezione brevettuale di questo metodo innovativo di mappatura degli stakeholder come "modello di business": una prima bozza essenziale di questo lavoro è stata pubblicata in data 09 dicembre 2010, in modalità copyleft. Il saggio riassumeva il "razionale" alla base del metodo, senza illustrare il metodo stesso nel dettaglio. Successivamente – dopo aver avuto contezza di alcune violazione del copyleft (citazioni e tentativo di utilizzo del metodo senza citare le fonte) – la clausola di protezione della prima versione del saggio è stata modificata da copyleft a copyright. Ancora successivamente, in data 29 novembre 2016, è stata presentata una richiesta di copertura brevettuale come modello di business allo US Patent Office, e contemporaneamente la versione presente online di questo articolo è stata arricchita di tutti i dettagli relativi al metodo, dettagli oggetto di richiesta di copertura brevettuale.
In data 31 maggio 2018 è stata infine concessa la patente di brevetto n° US2018/0150852-A1, e l'articolo è stato ulteriormente aggiornato.

Re BOX



L’ospite di questa settimana del mio blog è Marco Lei, co fondatore di Re Box.

Ciao Marco e benvenuto sul mio blog. Come e quando nasce Re Box?

L’idea nasce ad agosto del 2015 e lo stimolo è venuto da mio figlio Nathan che all’epoca aveva 9 anni. Una sera eravamo in un ristorante messicano e lui, come spesso accadeva, aveva avanzato la maggior parte di quanto ordinato nel piatto. Noi, come nella maggior parte dei casi, abbiamo chiesto di portare a casa quello che non era riuscito a mangiare e come spesso accadeva il tutto ci è stato consegnato in vaschette di alluminio all’interno di un sacchetto improvvisato. Quella notte mi stavo addormentando e mia moglie Daniela scuotendomi: “Marco, ma visto che in molte nazioni è una pratica consolidata e qui non esiste ancora, perché non facciamo noi la “doggy bag” italiana?”. Io ho borbottato qualcosa di incomprensibile. A questo punto lei si è addormentata, io ho passato la notte guardando il soffitto. Alle 5 di mattina mi sono alzato e con forbici e cartoncino è nato il primo prototipo di quella che sarebbe diventata la nostra reFOOD. Successivamente poi nasce anche la reWINE per portare a casa la bottiglia di vino aperta ma non terminata.

In questa fase il vostro pubblico di riferimento sono i gestori dei ristoranti. Che tipo di risposte state ricevendo?

Diciamo che la nostra reFOOD si porta dietro una cultura che in italia non è ancora molto consolidata, la difficoltà principale è far capire al ristoratore che son sempre di più le persone che avrebbero piacere di trovare questo tipo di servizio. L'altro aspetto è il senso di vergogna che l'italiano medio prova nel chiedere di portare a casa quello che non ha terminato. Ormai è risaputo che per il motivo principale di questo blocco è dato dal prodotto. Più del 70% degli italiani sarebbe disposto ad adottare questo atteggiamento se gli venisse proposto un prodotto bello, comodo e pratico per poterlo fare; e non la classica vaschetta in un sacchetto della spesa. Per questa estate i ristoranti che avranno la nostra reFOOD arriveranno a 400 in 33 province e diventeranno 800 entro fine anno.

Possiamo affermare che, come dimostrano numerose ricerche, cresce la consapevolezza delle persone che il cibo non si spreca. Come vedi il futuro della sostenibilità?

Ormai siamo arrivati ad un punto tale che l'attenzione verso la sostenibilità è diventata una priorità assoluta, non possiamo più procrastinare. Dobbiamo passare dalla modalità "moda" alla modalità "fare". Non basta dichiarare di voler fare, sventolare bandiere per salvare il pianeta. Bisogna che ogni singolo individuo cominci ad adottare anche piccole attenzioni che però sommate nel tempo possano veramente invertire una rotta decisamente catastrofica. "There is no a Planet B" scrivono, e così è. Il nostro progetto parte proprio da queste considerazioni e basi. É chiaro che il cibo che possiamo "salvare" con le nostre reFOOD non possa risolvere il problema degli sprechi alimentari che si manifesta per più del 50% nell'ambiente domestico, ma è un lavoro culturale sulla singola persona. Se riusciamo a convincere e ad abituare le persone a fare quel piccolo e semplice gesto probabilmente cominceranno a vedere quanto non terminato non più come un qualcosa da buttare via ma come una risorsa. Nel momento in cui avviene questo cambiamento di visuale anche all'interno della propria casa o in altre situazioni l'atteggiamento generale verso il cibo dovrebbe cambiare.

Quali sono i vostri programmi di sviluppo?
Vista la difficoltà, in questo momento storico, di far comprendere direttamente ai ristoratori la cultura che la nostra reFOOD si porta dietro abbiamo deciso di cominciare a lavorare con le Amministrazioni Comunali strutturando dei progetti sul territorio dove andiamo a lavorare proprio sulla divulgazione della cultura: con i bambini nelle scuole, con i loro genitori, con le associazioni sul territorio e con i ristoratori. Tutto questo mettendo in campo dei contest e dei premi al fine di incentivare degli atteggiamenti virtuosi verso il cibo.
Dopo l'estate dovrebbe partire anche una campagna di *equity crowdfunding* per aumentare l'impatto sia commerciale che culturale e per cominciare a pensare all'internazionalizzazione dei nostri prodotti.

Traffico esseri umani, il tech fa muro



Tech against trafficking è l'associazione fondata da BT, Microsoft e Nokia per la lotta al traffico di esseri umani

attraverso la tecnologia. Insieme all'Onu, nel 2018 hanno iniziaito a monitorare e lavorare su soluzioni tech per lo sviluppo di una strategia triennale

Il **lavoro forzato** e la **tratta di esseri umani** colpiscono circa **40 milioni di persone**in tutto il mondo. Un problema diffuso e complesso da affrontare, come ha descritto anche l'ultimo rapporto del dipartimento di Stato Usa presentato a fine giugno. Per cercare di affrontarlo nel modo più efficace, un gruppo di **aziende tech** insieme a **Onu** e l'organizzazione globale no profit **Business for social responsibility (Bsr)** si sono unite per lanciare "**Tech against trafficking**", progetto di collaborazione per creare **app e tool specifici** per queste tematiche. I membri fondatori sono **BT, Microsoft e Nokia**, che hanno promosso il dialogo su come la tecnologia può essere utilizzata al meglio per lottare contro la schivitù moderna, dialogo avviato un anno fa durante un evento di Wilton Park, forum internazionale dedicato alle discussioni su temi strategici del nostro tempo.
Ora la conversazione si è ufficialmente trasformata in azione. «L'evento del Wilton Park sembrava l'inizio di qualcosa di potente – ha commentato sul sito del Bsr **Eric Anderson**, responsabile del modern slavery program presso Bt – Ognuno si è rimboccato le maniche e ha preso appunti. È stato unico riunire diverse prospettive di esperti provenienti da aziende tech e gruppi della società civile di tutto il mondo. Quei tre giorni hanno rivelato le concrete opportunità di fare la differenza e una forte volontà di collaborare per riuscirci. Dovevamo trovare un modo per far sì che continuasse». «Abbiamo bisogno di collaborare più strettamente come industria e unire le forze con esperti nella lotta al traffico per fermarlo – ha incalzato **Laura Okkonen**, responsabile dei diritti umani presso Nokia – Insieme massimizzeremo l'**impatto positivo della tecnologia**».
I primi passi di tech against trafficking nel 2018 serviranno per **mappare e analizzare il panorama**delle attuali iniziative

incentrate sulla tecnologia per affrontare la schiavitù moderna. I **risultati chiave** saranno condivisi pubblicamente **entro la fine dell'anno per poi sviluppare una strategia triennale**. Le potenziali aree di interesse includono **app cloud** e **mobile** per consentire ai**soccorritori, alla società e ai lavoratori** di sensibilizzare, accedere alle risorse e segnalare problemi. **Hardware di base**, come laptop e smartphone più facilmente disponibili alle **Ong**. **Linee di assistenza nazionali** che aiutano le vittime e fungono da centri di raccolta dei dati. **Analisi di informazioni** e strumenti per affrontare il problema del sovraccarico di dati, utilizzando **AI e big data.** Strumenti di **trasparenza della supply chain** per migliorare la **tracciabilità** e la coerenza agli standard di lavoro.
«È grandioso vedere queste organizzazioni all'avanguardia nel loro impegno contro la schiavitù moderna – ha detto **Andrew Wallis**, direttore del centro anti-schiavitù Unseen –. Portano una quantità enorme di **esperienza tecnica,** oltre a un'enorme **influenza**. La tecnologia offre un potenziale di trasformazione non solo per **interrompere e ridurre** la schiavitù moderna, ma anche per sostenere i meccanismi di **cura e recupero** per i **sopravvissuti**».

Ci sono prove di un attacco degli hacker russi di APT28 anche in Italia



Lo sostiene una ricerca presentata dallo Z-lab di Cybersec: "Il bersaglio potrebbe essere la Marina italiana". La società di cybersecurity italiana ha incrociato i dati con analisti di una piattaforma aperta: si tratta del medesimo malware del gruppo legato al GRU, un software maligno che ha agito anche nell'hackeraggio delle mail democratiche nelle presidenziali Usa

Alla long story dell'interferenza della Russia nei processi elettorali occidentali, si potrebbe aggiungere un altro tassello. Questa volta la vittima sarebbe l'Italia. Ricercatori di un'azienda di cybersecurity italiana (CSE Cybersec) hanno scoperto che sulle reti italiane è circolato un malware in tutto simile a quello usato dai russi di Apt28 (aka Fancy Bear, o Pawn Storm), un gruppo paramilitare di hacker ritenuti collegati al GRU, il servizio segreto militare russo. Apt28 è stato a lungo ritenuto l'autore di tante operazioni molto importanti di hacking, tra le quali spicca l'hackeraggkio della primavera del 2016 ai danni delle mail del Comitato nazionale dei democratici, nella

corsa verso le elezioni presidenziali americane – prima che il nuovo indictment del Procuratore speciale Robert Mueller accusasse direttamente dodici ufficiali del GRU di aver eseguito, gestito e diretto l'operazione.
L'operazione di spionaggio – che i ricercatori chiamano "Operation Roman Holiday" – dura da alcune settimane, e non è certo chi sia la vittima dell'hackeraggio, ma potrebbe trattarsi della Marina italiana. Lo spiega Pierluigi Paganini, capo tecnologo di CSE Cybsec, che tra l'altro è direttore del Master in cybersecurity alla ormai famosa Link Campus University, intervistato da Agi: «Se adottiamo le logiche degli attaccanti parrebbe un riferimento alla Marina militare italiana e ci invita a verificare l'ipotesi che quel codice malevolo sia stato sviluppato come parte di una serie di attacchi mirati contro la Marina o altre entità ad essa associate, come i suoi fornitori».
Scoperta la "backdoor", la porta posteriore nelle reti, una serie di esempi del malware sono stati inviati da Cybersec a una piattaforma di cybersecurity aperta, Virus Total, attraverso un analista conosciuto online con il nome @drunkbinary. E da questo incrocio di verifiche è risultato confermato, spiegano i ricercatori, che esiste un pezzo di malware (il software maligno che di solito si impianta in un computer nemico, inducendolo a cliccare un link malevolo inviato alla vittima) in tutto analogo a quelli usati dagli hacker di Apt28.
Le somiglianze sono, dal punto d vista dell'evidenza informatica, molto rilevanti: il linguaggio in cui è scritto il codice del malware è uguale a quello di un malware usato dai russi (linguaggio Daphni). I luoghi remoti di command and control verso i quali vengono indirizzati i dati; anche alcune «librerie dinamiche" che il malware spinge surrettiziamente i computer attaccati a caricare. Non sarebbe il primo attacco russo contro l'infrastruttura italiana: di almeno un'altra circostanza è stato scritto già un anno e mezzo fa dal Guardian, che citò fonti governative, mai smentito da nessuno.
«Non possiamo escludere – sostiene Cybersec – che Apt abbia

sviluppato la backdoor per colpire specifiche organizzazioni, tra le quali la Marina militare italiana, o qualche altro subcontractor. Nelle nostre analisi non siamo riusciti a collegare il file malevolo dll ai sample di X-agent trovati, ma crediamo che entrambi siano parte di un attacco ben coordinato e chirurgico di Apt28». Varrà la pena notare che anche nel nuovo indictment di Mueller si racconta delle modalità X-agent con cui ha agito – in questo caso direttamente il GRU -contro le mail dell'ufficio di Hillary Clinton.

La ricerca, pubblica, è stata messa a disposizione sul sito dello Z-Lab di Cybersec. La piattaforma online che l'ha incrociata – VirusTotal – mette a disposizioni alcuni samples riscontrati. Cresce, negli ambienti degli analisti e degli osservatori internazionali, la preoccupazione che il caso Usa non sia affatto isolato. E inquietudini geopolitiche si sommano a quelle forensi: specialmente nel momento in cui il presidente americano Donald Trump, a Helsinki, ha detto di credere a Vladimir Putin, che nega che la Russia abbia hackerato le elezioni Usa, anziché a tutta la comunità dell'intelligence americana, che sostiene il contrario; e nel momento in cui il ministro dell'Interno italiano Matteo Salvini, incontrando a Mosca prima esponenti del Consiglio per la sicurezza nazionale russo, poi il ministro dell'interno russo, ha spiegato che l'Italia coopererà proprio con la Russia «nella cybersecurity e contro gli attacchi informatici», arrivando a scambiarsi – ha scritto Salvini – anche «banche dati» con Mosca.