Firefox Zero-Day Exploited to Deliver Malware to Cryptocurrency Exchanges

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/A7B5smE_PGM/firefox-zero-day-exploited-deliver-malware-cryptocurrency-exchanges

---

Welcome Italia, Winitalia, Palo Alto e Zurich lanciano il forum sulla cybersecurity

Avete mai visto cosa accade quando un hacker prende possesso del vostro PC aziendale e ruba indisturbato (e a vostra insaputa) tutte le vostre informazioni più preziose?

Vedere questa minaccia in azione con i propri occhi (con una simulazione realizzata da esperti naturalmente) è il modo migliore per capire a pieno la portata delle minacce alla cybersecurity.

L'occasione viene offerta dall'evento gratuito "**Cyber security Focus**" organizzato da **Winitalia** in collaborazione con **Welcome Italia, Palo Alto e Zurich.**

L'appuntamento è per domani, 21 giugno al **SeeBay Hotel** di **Portonovo** (AN) dalle 9:30 alle 13.

Il programma prevede seminari e incontri che permetteranno alle aziende e alle pubbliche amministrazioni di avere una panoramica dalla A alla Z sul tema della cybersecurity.

Adivisor internazionali ed esperti di **Welcome Italia, PaloAlto Firewall Training, Zurich, Westcon-Comstor**, saranno a disposizione per rispondere alle domande degli utenti.

Ecco alcuni degli argomenti che saranno trattati:

- sicurezza delle informazioni
- adeguamento alle normative (**GDPR**)
- prevenzione dalle minacce come virus e ransomware
- l'arte della cyber security in termini tecnologici e metodologici per le PMI e la pubblica amministrazione locale
- soluzioni per la sicurezza perimetrale ed interna basate sull'intelligenza artificiale
- piattaforme di cyber intelligence
- prevenzione assicurativa grazie alle nuove polizze sui cyber rischi pensate per aziende e pubblica amministrazione.

Durante l'evento si terrà un Laboratorio dal vivo "I cyber attack oggi e nel prossimo futuro" alcuni esempi di attacco e data breach con i laboratori di ethical hacking della Winitalia.

PROGRAMMA

09:30 Registrazione

09:45 Benvenuto ed inizio lavori

Federico Lombardi – Docente Cyber Security e ricerca blockchain presso Univ. Southampton

10:00 Sicurezza e affidabilità dei servizi di telecomunicazione

Samuele Sbacco – Welcome Italia

10:30 Deep Learning, quando l'intelligenza artificiale protegge le organizzazioni

Walter Doria – Palo Alto Networks

11:00 Coffee Break

11:15 Assicurarsi dai Cyber Rischi

Salvatore Finazzo – Market Facing Underwriter – **Zurich Italia**

11:45 Cyber Threat Intelligence: la tecnologia degli 007 per la sicurezza delle organizzazioni

Francesco Arruzzoli – Winitalia

12:15 Laboratorio dal vivo: I Cyber Attack oggi e nel prossimo futuro

EHG2 (Ethical Hackers Guardian Group) – Winitalia

13:00 Tavola rotonda e conclusioni

13:15 Fine Lavori

Per partecipare o avere maggiori informazioni clicca qui.

https://www.key4biz.it/welcome-italia-winitalia-palo-alto-e-zurich-lanciano-il-forum-sulla-cybersecurity/262401/

Florida City Pays $600,000 Ransom to Save Computer Records

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/hQchiwRqCtM/florida-city-pays-600000-ransom-save-computer-records

---

Cyberespionage Campaign Targets Android Users in Middle East

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/-GpL0rHFQ4s/cyberespionage-campaign-targets-android-users-middle-east

---

AMCA Files for Bankruptcy Following Data Breach

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Nno10Mq_NRc/amca-files-bankruptcy-following-data-breach

Firefox Zero-Day Vulnerability Exploited in Targeted Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/p26tPTHWeR0/firefox-zero-day-vulnerability-exploited-targeted-attacks

---

France Seeks Hacker for Trial Over Death Following Prank

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/ShN4p1tkpxo/france-seekshacker-trial-over-death-following-prank

---

Russia Says Victim of US Cyberattacks ‘for Years’

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/TG9MUhME46A/russia-says-victim-us-cyberattacks-years

La città di Baltimora vittima del ransomware RobbinHood. 18 milioni di dollari di danni

È passato poco più di un mese (7 maggio 2019 n.d.r) da quando l'intera infrastruttura informatica della città di **Baltimora** è caduta vittima di un massiccio attacco Ransomware di cripto-locking e ancora si contano i danni.

I funzionari locali, al momento, prevedono che l'attacco potrebbe superare il costo di **18 milioni di dollari** in attività di recupero e per il mancato guadagno, ma non è detto che questa stima sia definitiva considerato che è ancora in corso il processo di ripristino dei sistemi e l'indagine dell'**FBI** a riguardo non si è conclusa.

Le perdite

Le autorità al momento hanno suddiviso le spese in circa 10 milioni per recupero e spese forensi e circa 8 milioni di entrate fiscali e amministrative mancate.

L'attacco ransomware del 7 maggio, che, come detto, utilizzava codice cripto-locking maligno, ha colpito oltre 10mila computer all'interno della rete della città. Questo ha causato non pochi grattacapi al dipartimento IT che da settimane sta lavorando alla ri-autenticazione di tutti gli account legati alla città di Baltimora con nuove credenziali di accesso.

Fortunatamente polizia, vigili del fuoco e gli altri servizi

essenziali sono rimasti in funzione, ma la città sta ancora avendo problemi di accesso ai sistemi che controllano il parcheggio e le violazioni del traffico. Problemi sono stati registrati anche nel ciclo di fatturazione per il dipartimento che ha in carico la gestione delle acque pubbliche e addirittura per altre sezioni i processi si sono ridotti a carta e matita fino a quando i servizi IT e i dati di backup sono ripristinati.

Oltre al recupero e al lavoro forense, l'attacco rimane sotto indagine da parte dell'FBI, ed è probabile che un rapporto finale sia completato entro la fine di giugno.

Un indiziato principale: RobbinHood

Baltimora, secondo fonti interne, è stata vittima di **RobbinHood**, una variante relativamente nuova di ransomware che ha fatto il suo grande debutto in vari incidenti a partire dall'inizio dell'anno e che si rivolge principalmente alla Pubblica Amministrazione. Negli Stati Uniti aveva già colpito **Greenville** in North Carolina.

Non si sa molto sulla persona – o più verosimilmente sulle persone dietro – RobbinHood anche se alcuni ricercatori che hanno analizzato il ransomware si sono resi conto di come questo imiti il metodo di estorsione di SamSam, ma con un carico utile diverso e un attacco lato server non del tutto speculare.

Uno dei ricercatori che si sono presi in carico l'attività di analisi di questo fenomeno ha notato notato che RobbinHood può impattare oltre 150 servizi di **Windows**, tra cui l'anti-virus, i database, i server di posta oltre a tutti quei programmi dove potrebbe essere bloccata la crittografia. Il ransomware, inoltre, disconnette anche tutte le condivisioni di rete, il che permette all'aggressore di colpire le singole macchine.

Per **Adam Kujawa**, direttore di **Malwarebytes Labs** la maggior

parte delle scansioni di questo ransomware non mostrano nulla di speciale rispetto ad altre famiglie di che sono apparse negli ultimi anni. Per Kujawa il motivo per cui continuiamo a vederlo potrebbe essere dovuto agli attori che lo hanno sviluppato – o creato a partire dal codice sorgente di altre famiglie di ransomware – focalizzandosi su obiettivi che ricevono molta più attenzione nei media.

Pagare o non pagare

Come riscatto gli aggressori hanno chiesto **13 bitcoin**, o circa 100.000 dollari a prezzi correnti, per decriptare tutti i file dell'infrastruttura di Baltimora. Gli aggressori hanno anche deriso i funzionari della città attraverso un account **Twitter** ormai chiuso.

Il sindaco di Baltimora **Bernard C. Young** ha rifiutato di pagare e ha pubblicato un video che giustifica le sue ragioni al pubblico.

Anche a margine della conferenza stampa indetta durante l'insorgere dell'emergenza Young e altri funzionari hanno notato come l'FBI stessa avesse consigliato alla città di non pagare – anche se va ricordato che gli esperti ritengono che non pagare non sia sempre la risposta giusta –. Secondo questi infatti il metodo migliore è sempre e comunque la remediation, laddove questo non possa essere rapidamente imbastito potrebbe essere più facile ed economico negoziare. La chiave è avere un piano di "contingency" in atto molto prima che l'attacco avvenga.

Predisporre di una strategia difensiva preventivamente può essere la chiave per sopravvivere o ridurre al minimo gli impatti degli attacchi.

EternalBlue o qualcosa di nuovo?

Oltre ai regolari aggiornamenti sull'evolversi della situazione pubblicati dalla giunta di Baltimora, ci sono stati diversi rapporti tecnici pubblicati nelle settimane a seguito dell'attacco che si interrogavano se l'attacco ransomware di Baltimora sia stato il risultato della vulnerabilità di EternalBlue ancora presenti in molti dispositivi Windows

Secondo il **New York Times**, gli aggressori dietro RobbinHood hanno utilizzato la vulnerabilità **EternalBlue** (sviluppata dalla U.S. National Security Agency e poi rilasciata online da un gruppo chiamato ShadowBrokers).

Da allora, gli aggressori hanno usato gli exploit per sfruttare questa vulnerabilità e per diffondere ransomware – incluso **WannaCry** –.

Alcuni hanno sostenuto che il governo federale debba assumersi la responsabilità per i tipi di attacchi che colpiscono Baltimora e altre città da quando l'**NSA** ha sviluppato gli exploit.

Ci sono stati anche tentativi in senso opposto, per spegnere le fiamme, sostenendo che Eternal Blue non abbia nulla a che fare con l'attacco.

Va detto che anche chi ha seguito da vicino la vicenda crede che EternalBlue non sia mai stato usato contro Baltimora, ma che un attacco di spear phishing focalizzato sui dipendenti della città sia stato il probabile punto di infezione iniziale.

A seguito di questa prima violazione gli aggressori hanno potuto muoversi lateralmente attraverso la rete manipolando il PSExec di Microsoft, uno strumento di amministratore legittimo, prima di cercare i file da cifrare.

Amministrazioni locali sotto attacco

Ciò che l'incidente di Baltimora dimostra è che le città sono sempre più spesso vittime di ransomware. A maggio, una società di sicurezza a questo proposito ha pubblicato uno studio che ha rilevato 53 diversi attacchi di ransomware contro le amministrazioni locali nel 2018, e almeno 21 incidenti separati quest'anno.

Le ragioni per cui gli aggressori prendono di mira i governi locali variano, ma la motivazione più assodata è che questi approfittino di tutte le opportunità disponibili e spesso a livello locale l'attenzione alla sicurezza è nettamente più bassa.

Gli attacchi, quindi, continueranno. I Criminal Hacker inseguono bersagli di opportunità più di ogni altra cosa, il che significa che potrebbe non essere stato uno sforzo focalizzato quello per infettare Baltimora, ma dopo aver sparso una quantità di e-mail ad una serie di indirizzi associati al Governo, qualcuno ha abboccato l'esca.

Per questo motivo è facile ipotizzare che gli attacchi non accenneranno a diminuire, fintanto che ci sono reti vulnerabili agli attacchi sia attraverso falle di sistema sia attraverso errori dell'utente.

Approntare una difesa

È uno scenario senza uscita?

Ovviamente no, ma l'azione deve essere duplice.

Come ha dimostrato Baltimora al momento le due principali criticità di cybersecurity sono legate al lato tecnico, ma anche a quello umano.

Su questo secondo fronte l'azione deve avere due direzioni: bisogna lavorare sull'awareness dei dipendenti statali, soprattutto nei confronti delle minacce più comuni e al contempo c'è necessità di formarli…

Per assolvere questa duplice funzione si possono sfruttare i servizi di **Phishing Simulation Attack.** La soluzione permette alle aziende e alle amministrazioni di contrastare questo fenomeno attraverso un test dello human factor e garantendo anche una efficace attività di training e awareness. Il servizio adotta lo stesso modello di un attacco standard (di fatto simulandolo) permettendo di misurare il livello di esposizione al rischio phishing aziendale e al contempo effettua una attività di formazione e awareness efficace dei dipendenti. È riduttivo sottolinearlo, ma anche le misure più efficaci di Cyber difesa si possono rivelare inutili se in azienda le persone continuano a cadere vittima di questi inganni.

Sul lato più tecnico è fortemente consigliato a tutte le organizzazioni di approntare un Data Breach Incident Response Plan, l'unica soluzione che permette di adempiere a ciò che stato normato all'intero del GDPR.

Il servizio permette di:

- **stabilire** quali dati sono stati compromessi;
- **formalizzare** lo stato delle misure di sicurezza in essere;
- **predisporre** il piano di remediation.
- **gestire** l'incident e supportare l'azienda nel ripristino delle attività;
- **analizzare** la natura della violazione;
- **identificare** le evidenze, le prove e le informazioni tecniche;
- **determinare** la tipologia dei dati compromessi;

Nel dettaglio il processo si svolge in cinque fasi ben

strutturate: Si parte dalla **Cyber security investigation**, il primo step che ha come obiettivo l'identificazione dei vettori d'attacco, dei punti d'ingresso, dei target colpiti e delle tecniche usate per portare a fondo l'assalto. Questi dati si evincono grazie all'attività di log analysis, tracking dell'attacco, target analysis e data compromise discoveries.

L'output di queste attività viene trasformato in un executive summary e un technical report, facilmente consultabile. Fa seguito la **Forensic investigation,** questa ha come scopo la cristallizzazione delle evidenze legali e delle prove raccolte tramite computer e altri device. L'obiettivo è di esaminare i dispositivi digitali seguendo processi di analisi forense al fine di indentificare, preservare, recuperare e analizzare i dati raccolti. Anche in questo caso vengono resi disponibili un executive summary e un technical report oltre alla copia forense.

Lo step successivo è l'**ICT integrity checkup, la** fase di verifica dell'integrità della struttura. Questa consiste nel controllare e verificare se all'interno dell'infrastruttura non siano presenti elementi malevoli installati dagli attaccanti. L'intero step viene portato a termine attraverso assett inventory, malware assessment e ICT assessment. La produzione è, come prima, di un executive summary e un technical report. Finito questo si passa al **Vulnerability checkup che** ha lo scopo di preservare l'integrità dell'infrastruttura informatica. Un'analisi delle criticità che ha l'obiettivo di identificare e determinare le eventuali vulnerabilità sfruttate da terze parti per un possibile attacco a livello di infrastruttura esposta su internet e infrastruttura interna. Tutto ciò avviene mediante penetration test, vulnerability test e network scan. Anche qui viene fornita documentazione completa.

Infine ha inizio il **Reporting/remediation plan.** La fase conclusiva ultima fase consiste nel redigere la documentazione relativa alle informazioni necessarie per la completa e

corretta compilazione della notifica al Garante oltre a fornire indicazioni di dettaglio per la corretta security governance aziendale. Questo avviene attraverso attività di report e remediation plan. Il risultato è l'intera overview della tipologia dei dati compromessi, l'elenco di questi, la metodologia e la modalità dell'attacco, i target vittime, le misure di sicurezza adottate e la creazione di un security remediation plan.

Se Baltimora, con i suoi 600mila abitanti è rimasta paralizzata o comunque danneggiata per qualche settimana, gli effetti sulle città metropolitane più grandi potrebbero essere n volte più gravi. Le soluzioni ci sono, l'unica cosa che rimane da sconfiggere è la reticenza a portarsi in linea con le best practice di cybersecurity.

https://www.key4biz.it/la-citta-di-baltimora-vittima-del-ransomware-robbinhood-18-milioni-di-dollari-di-danni/262064/

L'attacco a Telegram durante le proteste a Hong Kong. Cos'è accaduto?

Telegraph, Telescope, la sicurezza dell'App e tutte le novità dell'ultimo update di Telegram alla versione 5.7: di questo, in sintesi, abbiamo parlato nelle scorse due puntate della nostra Guida a Telegram, qui e qui. Siamo a buon punto del nostro percorso. È ora di iniziare a tirar le fila e trarre alcune conclusioni.

Prima, però, facciamo una breve incursione nell'attualità, per dare conto di una news, comunicata da Telegram via Twitter lo

scorso 12 giugno, nonché confermata sempre con un tweet dallo stesso Pavel Durov, a seguito delle proteste tenutesi in questi giorni a Hong Kong. Come ben riportato poi da TechCrunch, l'App, infatti, ha registrato per l'occasione pesanti attacchi ed è andata in tilt per un attacco DDos. Che cos'è accaduto, esattamente?

I residenti della città-stato hanno utilizzato l'App per organizzare le proteste contro la legge sull'estradizione e sfuggire così alla sorveglianza. Nel dettaglio, Telegram è stata usata per coordinare le manifestazioni contro la nuova legge sull'estradizione e sfuggire alla sorveglianza di Pechino, proprio grazie alla sua sicurezza e al suo sistema crittografico, che la rende particolarmente utile in questi casi. L'App, però, è stata presa di mira da alcuni cyber criminali e ha smesso di funzionare. Pavel Durov ha detto che gli attacchi sono partiti dalla Cina e che non è la prima volta che deve far fronte a queste operazioni di ostacolo. Era già successo in passato, sempre in coincidenza con una protesta nella città autonoma che era stata coordinata tramite l'App.

Attacco DDos

L'attacco informatico che ha colpito Telegram è di tipo **DDos**, acronimo di *Distributed Denial Service*. Questo tipo di offensiva tenta di rendere impossibile l'erogazione di un servizio internet generando un numero molto alto di richieste, così da saturare il server e renderlo instabile. Per fare capire agli utenti che cosa stesse succedendo, Durov ha usato una metafora: «Pensate che un esercito di lemming abbia appena saltato la fila del **McDonald's** di fronte a voi e stia ordinando un whopper (il panino di punta di Burger King). Il server – cioè i camerieri – sono impegnati a spiegare ai lemming che sono andati nel posto sbagliato, ma ce ne sono così tanti che il server non può più prendere il vostro ordine».

TechCrunch ricorda che Telegram è stata attaccata anche quattro anni fa: in quel caso, era stato bloccato soprattutto l'accesso alla versione web dell'App, e le persone che vivevano nella Mongolia interna, nella provincia di Yunnan, Heilongjian, e a Shenzen e Pechino, non riuscivano ad utilizzarla. Allora, Durov non disse chi c'era dietro quegli attacchi, ma solo che provenivano dall'Asia orientale: si sospettò, però, della Cina. In quel periodo infatti Pechino aveva accusato alcuni avvocati di diritti umani di attaccare il Partito comunista e il governo, e uno di loro era stato costretto a confessare in televisione che «molte attività erano state pianificate e organizzate» su Telegram. Zhai Yanmin, l'avvocato, in quell'occasione aveva spiegato che gli avvocati si erano scambiati informazioni grazie alle Chat segrete.

In breve, comunque, tutto è tornato alla normalità. Riprendiamo, dunque, il filo del nostro discorso e cerchiamo, come anticipato, di trarre le prime conclusioni.

Telegram, *Who*, *What*, *Why*. Che cos'è, per chi è, il primo *perché*

In principio abbiamo presentato Telegram come «Il braccio operativo di *#HelpMarketing* e *#Digital #Education*», *lo* strumento *par excellence*, il modello esemplare di un «Digitale Utile» che sprigioni tutto l'«Utile del Digitale». Un'App che, per caratteristiche intrinseche, massimamente si presta a essere *usata bene*, in modo «digitalmente educato»: *bene per il* bene, con responsabilità, consapevolezza, etica e, dunque, proficuità.

1. ***#What*? Fatto!**

Ora che abbiamo conosciuto la città, le sue piazze e

quartieri, i vicoli nascosti o almeno quelli principali e, soprattutto, i suoi abitanti, cittadini, personaggi, auspichiamo che appaia confermata l'«utilità»di Telegram, che come tale *porta all'Utile*, fa *l'Utile* con l'Utilità. Telegram *aiuta*, nella pluralità dei suoi sensi, per il suo equilibrio tra **velocità e sicurezza**, il **valore unico del network** che si viene a creare, un **rapporto qualità-prezzo** e una **convenienza** irrintracciabili altrove nella relazione tra investimenti, sforzi fatti e risultati ottenuti. Per questo, dunque, pare davvero mostrarsi come la piattaforma ideale ove implementare una strategiadi successo, che conduca al raggiungimento dei propri traguardi nel business e nella vita.

Abbiamo dunque così risposto alla domanda sul ***#What***, sul «che cosa» sia Telegram, non solo in senso manualistico – d'illustrazione delle sue *features* fondamentali, passaggio peraltro necessario per i neofiti che non conoscano ancora l'applicazione – ma in un'ottica più profonda di chiarificazione della sua natura e «vocazione»?

Quanto all'aver dato una risposta esaustiva, certamente no: auspichiamo però di aver iniziato a far pulizia delle prime ombre e a puntare più chiare luci su uno strumento del digitale ancora troppo ignorato, specie paradossalmente quando si pensa di averlo compreso e s'inizia a usarlo. Male.

- ***#Who*? Fatto!**

Telegram è *per chi* cerca *la* risposta, la soluzione al problema chiave di tutti noi. Come fare business oggi, cioè, pur in tempo di crisi – in un'innovazione «liquida», fluida e continua difficile da cavalcare – come raggiungere il successo, i propri traguardi e obiettivi, nel lavoro e nella vita. Ecco la nostra prima risposta al ***#Who***, al «chi» può maggiormente beneficiare di Telegram: *tutti* potenzialmente, in ogni settore, sul pianoprofessionale e personale. Massimamente, poi, **imprenditori, manager, liberi professionisti** che, nella piattaforma, possono trovare

l’occasione di **fare business a costo (quasi) zero**.

- ***#Why*? Fatto! Almeno in parte…**

Ancora, quanto visto sin qui su tipologia di messaggi, *Cloud Chats*, *Secret Chats*, crittografia in Telegram – nelle sue due forme *client-server/server-client* da un lato ed *end-to-end* dall’altro, in una distinzione di livelli non casuale ma con un obiettivo preciso – e infine su Gruppi, Supergruppi, Canali e Bot, ha mostrato come le caratteristiche dell’App, volute e difese *in primis* tuttora dal suo fondatore, già siano sufficienti a sciogliere il nodo del ***#Why***, del nostro «primo perché»: perché, cioè, usare Telegram il suo valore in senso *assoluto*, anche a prescindere da particolareggiate comparazioni con i competitors e da un suo inserimento nel contesto storico, nell’epoca – digitale e non solo – in cui viviamo.

Telegram, già così, si confermerebbe come l’App, il territorio ideale, sul piano professionale e personale, sociale, istituzionale, educativo, del mondo dell’informazione, per garantire:

- **Velocità**e**sicurezza**;
- **Valore unico del network creato**;
- **Niente barriere all’ingresso**. Si tratta diun**progetto non commerciale, gratuito**;
- **ROI al 100%**, **rapporto unico qualità-prezzo**, ottimizzazione della relazione tra risorse investite, economiche e non solo, e risultati raggiunti: **il *tutto per tutti* a costo zero**.Senza ticket da pagare diretti o indiretti, né in termini di «compromessi personali» – come con la cessione dei propri dati, una costante degli altri social o molte altre App – né di investimenti economici da sostenere ad esempio in #SocialAds. Una massimizzazione del risultato col minimo sforzo: economico, di accessibilità, fruibilità, universalità nella diffusione dei contenuti.

- **Telegram, un vero *earned media* (l'ultimo rimasto?).**

Qui fiducia e successo te li guadagni sul campo, con olio di gomito – ma se lavori bene, se la *usi bene*, il dollaro, il ROI, arriva. Quell'*earned media* che avrebbe dovuto essere Facebook, con la sua promessa di «connettere il mondo» – promessa riproposta anche a tredici anni dalla sua nascita, nel febbraio 2017, col Manifesto *Building Global Community*, promessa invece sempre più tradita – e trasfiguratosi in breve in *paid media*.

Un *earned media* che verrebbe quasi da definire *owned media*, «proprietario», tanto grandi sono l'apertura, la libertà di personalizzazione di ogni utilizzo dell'App e delle strategie di comunicazione attuabili grazie ad essa.

- #YouTelegram, Telegram Utile-Per-*Me*.

#YouTelegram, ci è venuto così da ribattezzare l'App, sulla scia della nota ***Youtility***, la **utilità-per-te** di **Jay Baer**, cifra di quel che sono solita chiamare **#HelpMarketing**, **Marketing dell'Aiuto**, della **Responsabilità**: un «Marketing del volontariato», egoisticamente altruista, altruisticamente egoista, «tanto utile che la gente farà la fila alla tua porta» per comprare da te. Un *Marketing del Cuore* che, se farai un uso intelligente dell'App con tutti i conseguenti benefici, saprà «venderti un **sogno via robot**»: tanto splendido che tu, cliente, non potrai non volerlo comprare da me.

Pavel Durov e il suo «Ferragosto di fuoco»

Anche Durov non mancò di ribadire questi concetti in un celebre post, «da scuola» ed esemplare, lanciato nel Ferragosto di ormai quasi due anni fa. Quale? E che cosa sosteneva, esattamente? Lo vedremo nella prossima puntata della nostra Guida.

https://www.key4biz.it/lattacco-a-telegram-durante-le-proteste-a-hong-kong-cose-accaduto/261971/