Telegram e l'arroganza dei governi

Roberto A. Foglietta
GNU/Linux Expert and Innovation Supporter

Published Aug 26, 2024

Articolo scritto a partire da post a loro volta scritti a partire da commenti che ho scritto su LinkedIn dal momento in cui si è diffusa la notizia dell'arresto in Francia del creatore di Telegram. L'articolo propone un'approfondimento anti-cronologico rispetto agli scritti e alle notizie pubblicate dalla stampa.

Telegram è il problema, vero?

> *La sicurezza delle reti è una priorità perché ignobili misfatti e crimini vengono compiuti ogni giorno grazie all'uso di Telegram. Coloro che invocano la libertà di parola sono complici dei criminali perché se non lo fossero non avrebbero nulla da temere (aka andrà tutto bene).*

È significativo in questo contesto citare il caso specifico dell'uso di Telegram per lo spaccio di cocaina a domicilio.

Prima di Telegram si usavano delle app specifiche potenzialmente ignote alle forze dell'ordine e sviluppate dai narcotrafficanti.

Queste app potevano contenere - e sicuramente accadeva - malware, spyware, etc. che metteva a rischio tutte le attività, dati e comunicazioni del cellulare stesso.

Insomma, non solo i cocainomani erano dipendenti dalla sostanza ma per poterla averla finivano per diventare essi stessi garanzia a favore dei narcos.

Mi si potrebbe rispondere: cavoli loro. Non proprio, visto che queste app erano installate anche negli smartphone dei portaborse dei parlamentari.

Basta infatti un'analisi delle acque reflue e degli scarichi fognari delle ali del parlamento per capire quanto questo "fenomeno" sia esteso e importante.

Certo la soluzione migliore sarebbe di censirli - grazie a Telegram - e convincere il governo a toglierli la patente finché il CERT non certifica che si siano disintossicati.

Il governo Meloni ha recentemente approvato una legge che permette di rifiutare i test anti-droga e alcolimetrici senza subire conseguenze [1].

Telegram è il problema, vero?

Note

- [1] Occorre precisare, come ha fatto notare un avvocato su LinkedIn, che in realtà è la Cassazione con sentenza n. 30041 del 23 luglio 2024 che ha permesso di giungere a tale interpretazione delle norme. Interpretazione che va in direzione opposta a tutte quelle che la stessa corte aveva emesso in passato. Quindi non è esattamente una legge specifica sull'argomento ma la conseguenza di una novità introdotta nella legislazione che ha portato a quel risultato e, per ragioni di efficienza, la novità va ricercata partendo dalle motivazioni di quella sentenza piuttosto che cercando fra la produzione legislativa recente.

28 aprile 2024 - Macron chiese nel 2018 a Durov di spostare la sede di Telegram a Parigi. - **lnkd.in/dZrd3xck**

Durante un pranzo nel 2018 con il fondatore del social, ma lui rifiutò la proposta. È quanto scrive il Wall Street Journal citando persone a conoscenza delle discussioni. Macron ipotizzò persino di concedergli la cittadinanza francese, secondo quanto riferito da una delle persone. Sempre secondo il WSJj, nel 2017 gli 007 francesi presero di mira Durov in un'operazione congiunta con gli Emirati Arabi Uniti che hackerarono il suo iPhone. La sicurezza francese era preoccupata per l'uso di Telegram da parte dello Stato islamico per pianificare attacchi.

Knowledge is the power, everything else is arrogance!

Telegram è open-source e il suo sviluppo è affidato a una ONG residente a Dubai. Ergo, se anche il suo fondatore riuscisse a convincere la ONG ad aggiungere backdoor o condividere le chiavi crittografiche - perché di questo si tratta - allora ci sarebbe un fork compatibile con la stessa rete ma con l'implementazione di sistemi di sicurezza atti ad evitare il controllo di terze parti.

Che per altro è già stato preventivamente fatto, parecchio tempo fa e infatti oggi, pur essendo meno diffuso questo fork è molto apprezzato.

D'altronde non si capisce perché mai si dovrebbe rinunciare alla libertà di parola [1] e alla privacy per poi trovarsi alla mercé del crimine organizzato di stampo governativo o malavitoso. Quando le tecniche di investigazioni tradizionali hanno già gli strumenti per assicurare i criminali alla giustizia ma tali strumenti non sono in grado di scalare per offrire un controllo di massa, però efficaci per investigare in una certa finestra di tempo, specifici soggetti sospettati di compiere delitti.

Oltre al fatto che limitare la crittografia ai soli usi militari esporrebbe le banche e le istituzioni. A solo uso governativo esporrebbe i cittadini. Palesemente l'Europa sta andando alla deriva nel confrontarsi con la libertà di opinione e l'attentato alla sinagoga in Francia è stato solo un fattore di accelerazione che ha spinto la Francia di Macron a combattere una guerra ideologica all'uso della crittografia.

Infine occorre ricordare che lo scopo del diritto NON è di eliminare il crimine perché eliminare il crimine significa eliminare l'essere umano (caino docet) o stravolgere la sua natura [2] nella sua essenza. Lo scopo del diritto è eliminare la necessità della vendetta offrendo giustizia. Ciò implica che la giustizia debba essere equa e relativamente rapida.

Cosa sarebbe un governo senza una giustizia equa
se non una spelonca di predoni? (cit.)

Non è la prima volta che in Francia prendono decisioni avventate, come portare la guerra in Libia per distruggere le speranze di un dinaro africano proposto da Geddafi che poi ha portato la Francia a perdere l'Africa con la beffa finale del Niger che ha nazionalizzato le miniere d'uranio.

Così si ritorna al titolo: la sapienza è potere, il resto è arroganza.

Note

- [1] la libertà di parola è stata recentemente difesa anche da Papa Francesco in una lettera dedicata all'importanza della letteratura, scritta dal capo di un'istituzione che ancora nel 1966 aveva un indice di libri proibiti, fa un po' effetto. - **lnkd.in/dZzAx5Dr**, **lnkd.in/em_XKP-W**

- [2] transumanesimo - modificare l'essere umano tipo inserendogli un chip nel cervello che gli impedisca di pensare e fare cose che siano sgradite al governo e quindi di fatto sottraendogli il libero arbitrio per costringerlo ad attore (pupazzo) ubbidiente di un sistema sociale (e.g. alveare).

INTERMEZZO PER LA RASSEGNA STAMPA

27 agosto 2024 - L'importanza di Telegram in Russia. - **lnkd.in/dxA8wh84**

I russi utilizzano Telegram per qualsiasi cosa, dalle comunicazioni di tutti i giorni a quelle fra i comandanti e i soldati che stanno combattendo in Ucraina: e la possibilità che Telegram possa chiudere del tutto o parzialmente, oppure che Durov garantisca qualche tipo di accesso alle autorità francesi a chat o conversazioni private, sta generando estese preoccupazioni.

Ad un certo punto appare chiaro che l'arresto di Durov sta diventato un boomerang politico per Macron e fra i vari tentativi di salvare le apparenze la stampa diffonde la notizia che Telegram sia d'importanza strategica per la guerra con la Russia - già perché ormai è chiaro che la guerra non è più condotta con lo scopo di difendere l'Ucraina - ma purtroppo anche questo tentativo appare semplicemente ridicolo.

Infatti i russi, e in particola Putin, sono così preoccupati che Durov non è stato ricevuto da Putin nonostante gli abbia chiesto un incontro pochi giorni prima di volare a Parigi, quando entrambi si trovavano in Azerbaijan. Infatti il volo che lo ha condotto a Parigi è partito da Baku.

Ovviamente, su questo arresto, ogni parte sta cercando di tirare acqua al suo mulino quindi sulla stampa si alternano le dichiarazione dei Russi - in difesa della libertà di parola e della liberazione di Durov, che ha anche la cittadinanza russa, nonostante nel 2018 proprio a causa di una questione simile Durov dovette lasciare al fratello la gestione di VK, il Facebook russo - a quelle degli ucraini che millantano lo smacco agli avversari e paventano la disfatta dell'esercito russo a causa dell'uso di Telegram.

26 agosto 2024 - Macron: l'arresto di Durov (Telegram) non è una decisione politica. La polizia francese: Durov è ancora in custodia perché non collabora. - **lnkd.in/dwbaNJJY**

26 agosto 2024 - La dichiarazione per la stampa della Procura della Repubblica di Parigi scritta in francese e inglese sull'arresto e custodia cautelare di Durov. - **lnkd.in/dXeKrGd4**

Non è politica, dice Macron ma invece sì

L'affermazione di Macron, troverà un ulteriore elemento di smentita due giorni dopo quando il Wall Street Journal pubblicherà un articolo circa un'incontro fra Macron e Durov nel 2018 che non andò come il presidente francese sperava.

Quindi, passiamo direttamente all'analisi della dichiarazione ufficiale alla stampa e quindi dei capi d'imputazione elevati, non necessariamente contro Durov ma eventualmente contro persona non identificata ma Durov è stato trattenuto perché "*non collabora*":

- *Complicité* (complicità) x N
- *Blanchiment de crimes* (riciclaggio di denaro)
- *Association de malfaiteurs* (associazione a delinquere)

Queste accuse sono tutte da provare però già così suonano ridicole. Per capirne il motivo occorre conoscere l'architettura - **lnkd.in/dTyeB_aU** - e il modello di sviluppo di Telegram.

Così possiamo affermare con una certa sicurezza che questi capi d'imputazione non sono direttamente contestati a Durov ma a una persona ignota e quindi hanno fermato lui perché non aiuta le investigazioni ad identificare tali soggetti, infatti:

- *Refus de communiquer* (rifiuto a collaborare) - non vi è modo di fornire quello che la Gendarmerie chiede a meno di mettere delle backdoor e fare un'operazione di questo genere in un software open-source (*) sarebbe un boomerang oltre che inutile per via dei fork.

Su queste tre invece Durov potrebbe avere dei problemi

- *Fourniture de prestations de cryptologie visant à assurer des fonctions de confidentialité sans déclaration conforme.*
- *Fourniture d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans déclaration préalable.*
- *Importation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans déclaration préalable.*

avendo anche passaporto Francese e Telegram è distribuito anche in Francia. Però la questione non è banale, infatti il creatore di Telegram (anche qualora fosse presidente di un'ONG residente a Dubai) può essere ritenuto penalmente

responsabile di decisioni che magari vengono prese collettivamente (e magari per statuto dell'ONG a maggioranza) e non per decisione arbitraria del presidente?

Le evidenze mostrano che arrestare Durov è stata una decisione politica IDIOTA e l'unica cosa che in Francia potevano fare era bandire Telegram dagli appstore Google e Apple. Così i francesi avrebbero scaricato Telegram da altri siti e sarebbero stati esposti a malware e spyware per la gioia anche della Gendarmerie e non solo, però.

INTERMEZZO PER LA RASSEGNA STAMPA

25 agosto 2024 - Telegram, l'arresto di Durov non ha senso in Europa: ecco perché. L'analisi giuridica di Agenda Digitale EU. - **lnkd.in/dzWe2a9X**

La Francia ha arrestato Pavel Durov, fondatore di Telegram, ma allo stato delle norme e della giurisprudenza sembra impossibile che in Europa il gestore di un servizio digitale globale possa essere considerato concorrente in possibili reati compiuti dagli utenti della piattaforma, al punto di subire un ordine di custodia cautelare per il fondatore

Nel caso di Telegram, l'iniziativa francese appara ancora più grave di quelle portate all'attenzione dei Giudici Comunitari e Italiani, sia perché evidentemente si tratta di responsabilità penale, sia perché la sensazione è che il processo che seguirà avrà ad oggetto la crittografia in sé, come strumento in grado di eludere determinati controlli.

Riportando alla mente, casi che hanno suscitato scalpore in passato, come quello dello sblocco di iPhone utili per le indagini ad opera dell'FBI, rifiutato dalla Apple, ed ancor prima la nota querelle.

24 agosto 2024 - Pavel Durov, cosa sappiamo dell'arresto del fondatore di Telegram. -**lnkd.in/dVVYsxD2**

La gendarmeria aeroportuale si è presentata con un un mandato di perquisizione dalla direzione nazionale della polizia giudiziaria francese emesso sulla base di un'indagine preliminare, riguardo al ruolo di Telegram in una serie di reati, dalla ricettazione allo spaccio di stupefacenti, dalle pedopornografia alla violenza online.

Secondo le informazioni raccolte da Tf1, l'esecuzione del mandato era legata alla presenza di Durov su suolo francese e giustificato dalla supposta mancata collaborazione con le autorità.

L'arresto di Pavel Durov fondatore di Telegram a Parigi

Fondamentalmente le autorità francesi ritengono Durov complice dei reati che si commettono tramite l'uso di Telegram (sistema di chat peer-to-peer con

comunicazioni cifrate end-to-end) perché non fornisce supporto agli investigatori nell'intercettare le conversazioni fra gli utenti del sistema di messaggistica.

In pratica, perché Telegram offre quanto promesso e l'azienda che lo distribuisce non inserisce backdoor. Perché appare chiaro che un sistema di comunicazione P2P con crittografia E2E può essere vulnerabile solo se ci sono backdoor inserite di proposito. Si potrebbe contestare che basterebbe trovare delle vulnerabilità 0-day. Ma non è così, nel senso che trovare tali vulnerabilità sarebbe come dire che il protocollo SSH non è sicuro.

Perché Telegram non è altro che un elenco telefonico dinamico creato dagli utenti. Come faccio a saperlo? Telegram è stata fondata nel 2013, la prima beta release di Whatsup è del 2009. A settembre 2006, in seno al master di tecnologie open-source stavamo sviluppando un client-server per scambiarsi messaggi. Ma la cosa non dovrebbe stupire visto che ICQ è nato nel 1997 e l'ultima release (chiusura del progetto) è stata rilasciata del 2022.

Ciò che serve a due o più persone per comunicare fra loro è un elenco in cui a partire dal un riferimento noto (nominativo, nickname, n. cellulare) sia associata una chiave pubblica e usare qualsiasi software che supporti la crittografia a chiave pubblica, come GPG, e qualsiasi sistema di comunicazione, anche l'e-mail.

Un passo ulteriore è usare la tecnologia alla base di eMule (2002) per fare a meno di usare un'infrastruttura server. Così si passa all'architettura di rete P2P dove solo pochi nodi geograficamente distribuiti mantengono la rete attiva nel caso di un down di massa dei clients.

In questo contesto accusare Pavel di non offrire collaborazione agli investitori creando delle back-door è fondamentalmente una lotta ideologica al concetto stesso di informatica come tecnologia piuttosto che come strumento di sorveglianza governativo.

Lo hanno arrestato perché lo ritengono filo-russo ma non è vero nemmeno quello visto che proprio a causa dello stesso tipo di richieste ha dovuto abbandonare il controllo di VK (Facebook russo) ed è anche a quello che i francesi puntano, ma invano.

Più che altro quello che li ha mossi in questa direzione e il motivo per il quale Pavel ha deciso di visitare la Francia riguarda il recente attentato alla sinagoga - **lnkd.in/dvgNY-Yt** - e quindi l'inevitabile reazione del Mossad.

Evento che avviene a pochi giorni dall'affondamento del veliero Bayesian - **lnkd.in/d4zXhXRr** - una tragedia che per molti aspetti ha ricordato quella avvenuta sul lago di Como e che coinvolse agenti dei servizi segreti italiani e israeliani del Mossad.

Evidentemente però i negoziati sull'offerta di collaborazione riguardo all'anti-terrorismo (ricordiamoci che Telegram ha sede a Dubai) non sono andati benissimo, o per lo meno non come previsto.

Ma che ultimamente le cose non vadano secondo i piani pare alquanto un deja-vù in cui quelli che erano i poteri forti finiscono per dimostrare solo prepotenza e inettitudine annegata in un mare di ignoranza e talvolta becera stupidità.

D'altronde o si usa il cervello per il compito che si suppone sia stato progettato o si sia evoluto oppure si usa la testa come martello. A quanto pare l'Agente Smith ripete se stesso e come nel video "Another Brick in the Wall" sceglie di fare il martello.

- *Banging their head against dark walls of a dark maze, amazing!*

21 agosto 2024 - Anti-Israel hackers have released troves of classified data: Haaretz. - **lnkd.in/dg6yUjS6**

'The leaks are likely the most severe in Israel's history -- an unprecedented looting of gigabytes upon gigabytes of information of all sorts,' says Israeli daily.

The attacks, which began on Oct. 7, 2023, have targeted a wide range of entities, from military and defense contractors to hospitals and government ministries. The scale of the breach has overwhelmed Israel's cyber-security infrastructure.