# Magecart Skimmer Poses as Payment Service Provider

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/ZiLMTedyM3I/magecart-skimmer-poses-payment-service-provider

---

# EU Adopts Powers to Respond to Cyberattacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/K4e5ZZ034fo/eu-adopts-powers-respond-cyberattacks

---

# Instagram, online su un database non protetto dati di 50 milioni di Influencer

Privacy e social network, ci risiamo. Dati di 50 milioni di utenti, per lo più di influencer e celebrità, sono stati trovati in un database allocato su un serve AWS, **Amazon Web Services,** senza alcuna password di protezione: chiunque poteva entrare e prelevare i dati.

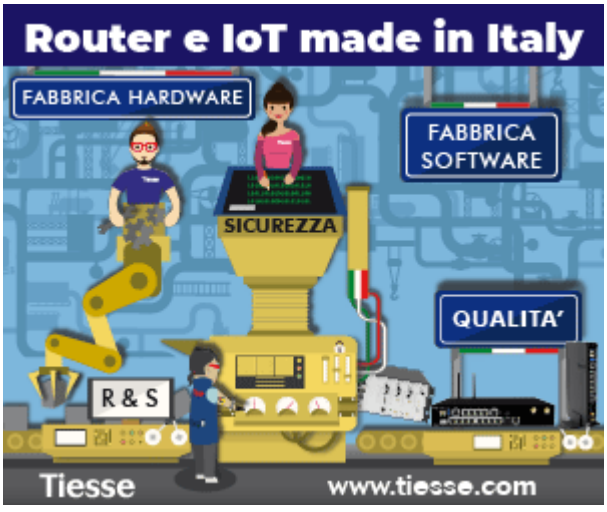
Un nuovo scandalo privacy proveniente dall'Universo **Facebook**,

in quanto **Mark Zuckerberg** è proprietario del popolare social network acquistato nel 2012 per la modica cifra di 1 miliardo di dollari.

A fare la scoperta è stata la testata americana **TechCrunch**, dopo essere stata allertata dal ricercatore **Anurag Sen.** Secondo quanto riporto dal quotidiano, l'archivio conteneva i dati di 50 milioni di utenti. Tra i dati che è possibile ricavare tutta la biografia dell'utente, la foto del profilo, il numero di follower, se sono verificati o no, la località (città e nazione) ma anche le informazioni di contatto private, come l'indirizzo email dell'account Instagram e il numero di telefono del proprietario dell'account.

## L'azienda proprietaria del database: Chtrbox

Il ricercatore, attraverso le sue rilevazioni, è riuscito a risalire al proprietario del database che è la società **Chtrbox**, con sede a Mumbai, che si occupa di social media marketing e che lavora proprio con gli influencer per pubblicare contenuti sponsorizzati sui loro account. E, infatti, tra i vari dati rintracciati, c'erano anche quelli riferiti alla capacità di influenza di ciascun influencer, in base al numero di follower, capacità di interazione, portata potenziale, "like" e singole condivisioni.



## Il secondo episodio in pochi anni

Il database è stato messo offline poco dopo la richiesta di spiegazioni dalla società indiana. Intanto da Facebook, un portavoce ha fatto sapere che la società sta esaminando il problema «per capire se i dati descritti, inclusi i numeri di e-mail e di telefono, provenivano da Instagram o da altre fonti.

Un episodio simile era già avvenuto un paio di anni fa, dopo che era stato scoperto un bug nelle **API** che aveva poi costretto la società di proprietà di Facebook ad attuare una stretta, in modo da limitare le richieste.

https://www.key4biz.it/instragram-online-su-un-database-non-protetto-dati-di-50-milioni-di-influencer/258812/

---

# TeamViewer Confirms It Was Hacked in 2016

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/w5hiix1uTI0/teamviewer-confirms-it-was-hacked-2016

---

# How to Evaluate Threat

# Intelligence Vendors That Cover the Deep & Dark Web

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/SAmYeEqkC4w/how-evaluate-threat-intelligence-vendors-cover-deep-dark-web

---

# User Data Exposed in Stack Overflow Hack

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Np8hHbe6iQ0/user-data-exposed-stack-overflow-hack

---

# Hacktivist Attacks Declined 95 Percent Since 2015: IBM

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/sywDsgEtT6U/hacktivist-attacks-declined-95-percent-2015-ibm

---

# Europol, smantellata la cyber-gang del malware GozNym

Hanno utilizzato il **malware GozNym** per cercare di rubare qualcosa come 100 milioni di dollari da oltre 41mila vittime. Con quest'accusa, una rete di cybercriminali è stata smantellata da un'operazione coordinata europea di polizia, secondo quanti riferisce ieri **Europol**.

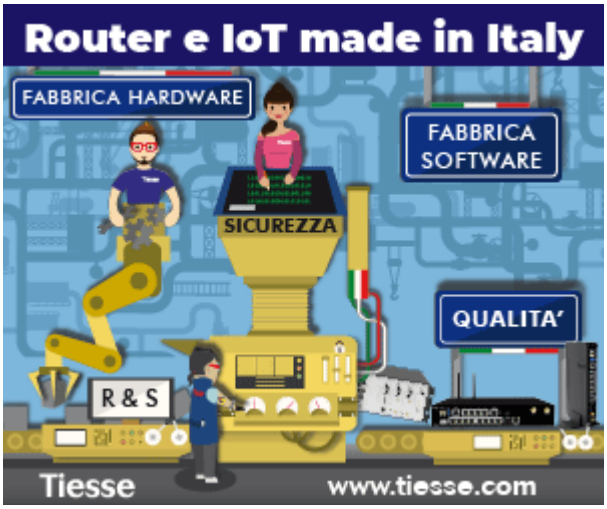
## L'indagine condotta in 4 Paesi

La complessa operazione di polizia è stata condotta negli Stati Uniti, in Bulgaria, Germania, Georgia, Moldova e Ucraina. Adesso dieci membri della gang devono rispondere negli Usa a una serie di reati, tra cui il furto di denaro e il riciclaggio attraverso conti bancari statunitensi e stranieri. Tra gli altri membri anche il 'capo' della rete, oltre al suo assistente tecnico, fermati in Georgia.

## 41mila computer infettati

La gang ha infettato 41mila computer con il malware, che ha catturato i dati bancari online per accedere ai conti correnti delle vittime.

La rete GozNym pubblicizzava le sue capacità di commettere cybercrimini come "un servizio". I componenti del network si presentavano come degli specialisti nel settore nei forum criminali online in lingua russa.




https://www.key4biz.it/europol-smantellata-la-cyber-gang-del-malware-goznym/258592/

---

# La crittografia di WhatsApp? Uno stratagemma di marketing

«Ecco perché WhatsApp non sarà mai sicuro». La denuncia, che segue all'ultimo scandalo dell'ennesima falla nell'App di casa Zuckerberg e della potenziale diffusione dei dati personali degli utenti, è arrivata direttamente dal Canale Telegram di Pavel Durov nella notte tra il 15 e il 16 maggio, rilanciando un articolo scritto di suo pugno su Telegraph che ha fatto scalpore.

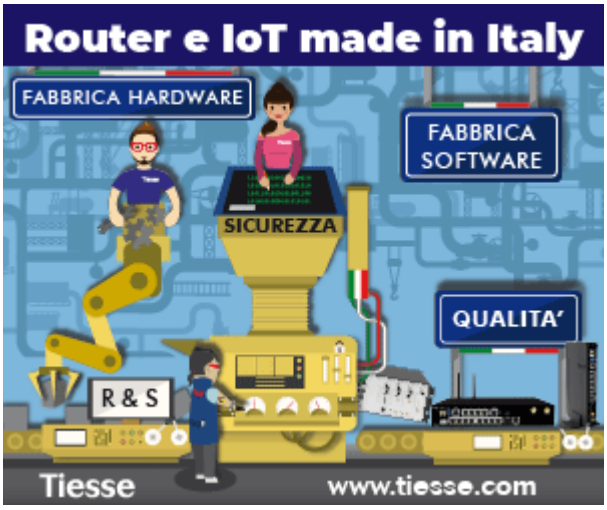
Perché? I punti ribaditi sono quelli da sempre caratterizzanti la filosofia di Durov nelle sue esternazioni circa il mondo Telegram in contrapposizione alle «lobby monopoliste e anti privacy» rappresentate per eccellenza da Facebook e WhatsApp. Due spunti però qui appaiono particolarmente significativi.

«In quasi sei anni di esistenza», spiega infatti Durov, «Telegram non ha avuto perdite di dati come invece WhatsApp ha di continuo. Negli stessi sei anni, Facebook e WhatsApp hanno

condiviso praticamente tutti i dati». E ancora: «WhatsApp ha aggiunto un po' di crittografia, ma è solo uno stratagemma di marketing. La chiave per decodificare i messaggi è disponibile per diversi governi, inclusi i russi».

# I fatti

Ricostruiamo anzitutto l'accaduto. 72 ore fa la notizia: «WhatsApp: "Falla nella sicurezza". Aggiornare l'App per battere il virus». La stessa WhatsApp, infatti, ammette di aver rilevato una vulnerabilità nel proprio sistema: una falla nella sicurezza che per settimane ha consentito agli hacker di installare *spyware* su alcuni telefoni e accedere ai dati contenuti nei dispositivi. Il software, scoperto a maggio, era in grado di installarsi nel sistema operativo attraverso le chiamate vocali, anche senza l'avvenuta risposta e senza lasciare alcuna traccia nella cronologia. La notizia, anticipata dal Financial Times, ha fatto il giro del mondo e la società, con un comunicato, ha invitato gli utenti – 1,5 miliardi in tutto il mondo – a scaricare «l'ultima versione dell'applicazione» e mantenere aggiornato il sistema operativo del cellulare come misura di «protezione».




Ripresa da quasi ogni testata e commentata da tutti i principali esperti del settore, non poteva non invitare a nozze anche il fondatore di Telegram, storico competitor che, giorno dopo giorno, aumenta la massa critica dei propri

utenti. I quali, pur essendo certo meno numerosi, vantano una fidelizzazione e una compattezza – in nome di principi quali libertà, democrazia, difesa della privacy, stop alla *Web Violence*, e di quel «progetto non commerciale, gratuito» che Telegram è e vuol restare sempre – che conferiscono loro un valore unico per chi opera entro l'App.

Ebbene, che cosa ha detto Durov? «Il mondo sembra scioccato dalla notizia che WhatsApp ha trasformato qualsiasi telefono in *spyware*. Non c'è però da meravigliarsi se i dittatori amano WhatsApp», esordisce. «L'App è liberamente disponibile in luoghi come la Russia o l'Iran, dove Telegram è bandito dalle autorità».

## Perdite e condivisione di dati

Continuando a leggere, ecco la denuncia di Durov: «In quasi sei anni di esistenza, Telegram non ha avuto perdite di dati come invece WhatsApp ha di continuo. Negli stessi sei anni, Facebook e WhatsApp hanno condiviso praticamente tutti i dati».

A che cosa si riferisce Durov? Nel dettaglio, Pavel rimanda a un dossier tutto da leggere sulle innumerevoli violazioni conosciute da Facebook e WhatsApp, sia per azioni hacker o per «volontaria» cessione dei dati ai Governi. «Dimentica falle, bug e backdoors», si titolava su Forbes già due anni fa, «questi sono i dati che WhatsApp e Facebook condividono regolarmente con la polizia e le autorità». «Quando *The Guardian*», si legge, «ha pubblicato un rapporto su una presunta backdoor di WhatsApp la scorsa settimana, questo ha suscitato sia timori di sorveglianza dello Stato sia di rabbia da parte di esperti di crittografia». Non è però un problema solo di violazioni: «Una delle maggiori preoccupazioni su WhatsApp dal punto di vista della privacy è la sua opacità, come spesso osservato nelle valutazioni della Electronic Frontier Foundation». E

l’allarme continua: «Se è vero che WhatsApp potrebbe non fornire il contenuto completo dei messaggi, il tipo di metadati che fornisce è spesso sufficiente per disegnare una mappa informativa della vita di una persona». Parola di Neema Singh Guliani, consulente legale presso l’*American Civil Liberties Union* (ACLU), che ha notato come WhatsApp condivida già le informazioni di contatto con Facebook, che possono essere fornite al governo. E l’informativa sulla privacy di WhatsApp rileva che memorizza alcune informazioni sulla posizione e sui contatti dove gli utenti hanno scelto di fornirle.

Potrebbe bastare questo a giustificare le parole di Durov: i casi, però, sul tema non si contano.

«L’anno scorso WhatsApp ha dovuto ammettere di aver avuto un problema molto simile: una sola videochiamata tramite WhatsApp bastava a un hacker per accedere ai dati dell’intero telefono». Lo scorso 12 ottobre 2018, infatti, la notizia: «Il servizio WhatsApp di Facebook ha annunciato di aver corretto l’ultimo bug sulla sua piattaforma che consentiva agli hacker di rilevare le applicazioni degli utenti quando rispondevano a una videochiamata in arrivo». Una notizia che seguiva di poco un altro scandalo, riguardante stavolta Facebook: coinvolto anche in quei giorni in una serie di problemi legati alla sicurezza e costretto ad ammettere una nuova violazione della sicurezza, che aveva colpito quasi 50 milioni di account proprio la settimana precedente.

Ancora, il 9 novembre scorso: «WhatsApp, attenzione alla versione web. Una falla permette di spiare le chat». «La popolare App, nonostante la crittografia end-to-end, non è così sicura come sembra e ci sono diversi trucchi per leggere le conversazioni altrui di nascosto, in modo semplice e gratuito», si leggeva. «Uno di questi è WhatsApp Web, la versione browser e desktop di WhatsApp. Basta andare su web.whatsapp.com dal proprio device, prendere lo smartphone della persona da spiare, aprire il suo WhatsApp e scansionare

il QR Code che appare sullo schermo, ricordandosi di lasciare la spunta “Resta Connesso”. In questo modo si vedrà, in tempo reale, con chi messaggia il partner e cosa scrive».

Ancora, il 22 febbraio scorso: «WhatsApp bug, scoperta una falla nella protezione Face ID e Touch ID». Che cosa era accaduto? «Un utente di Reddit, sito Internet di social news e intrattenimento, di nome de_X_ter, ha individuato unbug nel sistema di WhatsApp. Il riconoscimento biometrico con Face ID o Touch ID sembra non bloccare più l’accesso a eventuali intrusi. La falla individuata permette a chiunque di accedere alle chat di WhatsApp senza passare per il blocco del riconoscimento». Un bug riconosciuto poi dalla stessa società, passata subito a cercare la risoluzione, ma sempre in ritardo.

E ancora, il 10 agosto scorso: «Falla su WhatsApp, i messaggi già inviati possono essere modificati da chi risponde». «In queste ore», si scriveva, «WhatsApp si è mostrata scoperta nei confronti di un attacco malevolo battezzato FakesAppe individuato dagli israeliani esperti in cybersecurity di Check Point Software Technologies, che sono riusciti a sviluppare un codice in grado di modificare a piacimento quel che viene mostrato agli utenti di una conversazione all’interno delle risposte scritte attraverso l’apposita funzione *Rispondi*».

Di contro, la privacy di Telegram fa scuola, sia quanto a protezione verso possibili violazioni hacker, sia rispetto a possibili pressioni esercitate da governi e autorità. Sicurezza è parola d’ordine su Telegram e, infatti, esistono ben due diversi livelli di crittografia, di sicurezza e privacy, entrambe a prova di bomba:

La prima è quella utilizzata per le comunicazioni tradizionali, la seconda per quelle «segrete». «Supportiamo due livelli di crittografia», spiegano da Telegram: «la crittografia *server-client*, usata nelle Chat Cloud (private e di gruppo), mentre le Chat Segrete utilizzano un

ulteriore di livello di crittografia *client-client*. Tutti i dati, a prescindere dal tipo, sono crittografati nella stessa maniera – sia che siano testi, media o file. La nostra crittografia è basata sulla crittografia AES simmetrica a 256-bit, sulla crittografia RSA 2048 e sullo scambio di chiavi di sicurezza Diffie-Hellman». Abbiamo dunque, riepilogando, due diversi tipi di messaggi, ciascuno con differente livello di sistema crittografico, di sicurezza e privacy, garantite entrambe come inoppugnabili:

«Tutti i dati conservati sono protetti da una crittografia a prova di bomba», spiegano da Telegram qui, «e le chiavi di decrittazione, in tutti i casi, sono conservati in una pluralità sterminata di parti del mondo e nelle più diverse giurisdizioni. In questo modo ingegneri, sviluppatori locali, dipendenti, o, peggio, spioni online e offline non possono in alcun modo avere accesso ai tuoi dati». Nelle chat «normali» i dati sono «conservati», ma in modo tale – con un tale livello di crittografia e con quel loro quasi frantumarsi, come frammenti di cristalli, diamanti, nel globo, tra *data center* frazionati in ogni parte del mondo – che ne rende l'accesso praticamente impossibile a chiunque. Sono come porti di mari nelle cui acque subito si disperdono: oggetti che, all'istante, divengono ceneri al vento. Senza che nessuno legga i tuoi messaggi neppure volendo. Non ci sono casseforti, non ci sono chiavi. Nelle Chat segrete, poi, il livello di sicurezza è addirittura del mille per mille. Qui i messaggi non transitano da alcun server, mai. Neanche l'ombra, nemmeno per un istante, di una «cassaforte». O meglio: la cassaforte sei soltanto tu. La «chiave» la hai solo tu: tu e, naturalmente, la persona cui stai inviando quel tipo di contenuto. «Non c'è proprio nessun modo per noi o per chiunque altro, senza un accesso diretto al tuo *device*, di sapere che tipo di contenuto tu abbia mandato in quei messaggi. Noi non conserviamo le tue chat segrete sui nostri server», spiegano. «E comunque, dopo un breve periodo, non sappiamo neppure più chi o quando abbia mandato un certo messaggio in una chat

segreta. Per le stesse ragioni, le chat segrete non sono disponibili nel cloud: tu solo hai l'accesso a quei messaggi dal *device cui* – o *da cui* – hai inviato tali messaggi. Allo stesso modo, quando mandi foto, video o file via chat segreta, prima che tali contenuti multimediali siano caricati, questi sono crittografati con chiave separata sconosciuta al server. Tale chiave e il luogo del file sono poi nuovamente crittografati con chiave *ad hoc* e solo così inviati al tuo destinatario».

Questa è la massima forma di sicurezza e privacy che Telegram ti garantisce: come detto anche rispetto a Governi, autorità e spioni che vogliono indebitamente «farsi i fatti tuoi». Agli inizi dello scorso giugno si registravano attacchi russi anche su App Store: «Apple ha ceduto i dati degli utenti». Nel frattempo, lato Telegram, il movimento Digital Resistance programmava per il 5 giugno una manifestazione per la libertà su Internet. Il 17 aprile 2018 si registrava il sostegno a Telegram e al suo impegno per la difesa della privacy degli utenti persino da parte di Snowden: «Ho criticato la sicurezza di @telegram in passato», twittava, «ma la risposta di @Durov al totalitarismo del governo russo nel richiedere le chiavi a comunicazioni private – rifiuto e resistenza – è la sola risposta morale e mostra una reale leadership».

# La crittografia di WhatsApp? Uno stratagemma di marketing

Ecco, è questa forma di sicurezza e privacy che non troverai in WhatsApp, dove si parla sì di crittografia *end-to-end*, ma le cose stanno in maniera un po' diversa. E veniamo così alla seconda affermazione indicata come di particolare rilievo nel post di Durov: «WhatsApp ha aggiunto un po' di crittografia, ma è solo uno stratagemma di marketing: la chiave per decodificare i messaggi è disponibile per diversi governi, inclusi i russi».

Che significa? La risposta è semplice. L'impressione, se non la convinzione, è quella che i dati, una volta crittografati ad esempio su WhatsApp, vengano poi immediatamente disseppelliti dalla cassaforte ove erano stati racchiusi, presi da qualcuno che le chiavi le ha eccome, per essere poi immediatamente trasferiti in più sicure casseforti, in ben più inaccessibili centri di controllo, destinati ad analizzare quei dati, e dunque la tua vita online e offline, disegnando per te il destino di un tracciamento perenne, di una violazione della tua privacy senza fine, nella vita virtuale come in quella cosiddetta «reale».

Se hai ancora dei dubbi, leggi qui. Già a gennaio 2017, infatti, *The Guardian* lanciava l'allarme e lo riconferma ancora oggi: «Le *features* di progettazione di WhatsApp indicano che alcuni messaggi crittografati potrebbero essere letti da terze parti». All'epoca si segnalava nello specifico: «Il Security Code Change Notification online di WhatsApp afferma: "A volte i codici di sicurezza utilizzati nella crittografia end-to-end possono cambiare. Ciò è probabilmente dovuto al fatto che qualcuno ha reinstallato WhatsApp o ha cambiato telefono". Questa re-crittografia e ritrasmissione di messaggi precedentemente non consegnati potrebbe potenzialmente consentire a una terza parte di intercettare e leggere i messaggi non consegnati di un utente in una situazione in cui, ad esempio, hanno rubato la scheda SIM di un utente. Quando la terza persona ha inserito la carta SIM rubata in un altro telefono, è possibile quindi teoricamente raccogliere tutti i messaggi che non sono ancora stati consegnati all'utente in questione».

Una crittografia «bucata» o «perforabile» come questa non è paragonabile alla crittografia di Telegram. Anche Il Post commentando segnalava: «Il cambiamento della crittografia può consentire potenzialmente a WhatsApp di leggere i messaggi degli utenti. La vulnerabilità è stata scoperta da Tobias Boelter, un esperto di crittografia e di sicurezza informatica

della *University of California*, Berkeley, e il suo funzionamento è stato confermato da altri esperti». Boelter ha ulteriormente spiegato: «Se a WhatsApp fosse chiesto da un governo di rivelare i contenuti dei messaggi, questa lo potrebbe fare con il sistema di sostituzione delle chiavi di sicurezza». Boelter ha anche detto di aver segnalato la sua scoperta a Facebook nel 2016: l'azienda rispose di esserne al corrente e che era previsto che l'App si comportasse in quel modo. Sfruttando questo sistema, potenzialmente si potrebbero spiare intere conversazioni e non solo singoli messaggi: WhatsApp potrebbe per esempio farlo modificando il funzionamento dei server attraverso i quali passano i messaggi (senza essere poi salvati) per essere smistati e raggiungere il destinatario. L'articolo è stato, naturalmente, molto discusso e ha ricevuto repliche dalla società: le affermazioni contenute, però, continuano a essere centrali e decisive.

# Conclusioni

Non servono altre parole per mostrare la diversità di Telegram, da un lato, e WhatsApp & co. dall'altro, in tema di sicurezza e privacy, sia sul piano della vulnerabilità ad attacchi hacker, sia su quello della potenziale cessione a terzi dei dati degli utenti, dimostrata negli ultimi sei anni, come indicato da Durov, e da un'analisi distaccata della «crittografia» di WhatsApp: «mossa di marketing» in quanto cassaforte di cui, però, non tu ma altri hanno davvero le chiavi. La riflessione migliore ci pare, ancora una volta, quella conclusiva di Durov: «Noi di Telegram dobbiamo riconoscere la nostra responsabilità nel formare il futuro. La scelta è fra noi o il monopolio di Facebook. Tra libertà e privacy o avidità e ipocrisia. Li abbiamo già battuti una volta, nell'Europa orientale. Li batteremo di nuovo nel mercato globale della messaggistica. Dobbiamo». E ancora: «L'epoca dell'avidità e dell'ipocrisia finirà», scrive. «Inizia un'era di libertà e privacy. È molto più vicino di quanto sembri».

https://www.key4biz.it/la-crittografia-di-whatsapp-uno-stratagemma-di-marketing/258408/

---

# Stack Overflow Discloses Security Breach

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/TwAE3Fs4b4w/stack-overflow-discloses-security-breach