Varenyky: è arrivato il “trojan a luci rosse”

Ago 09, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, Phishing, Privacy, RSS 0

Individuato in Francia, il malware controlla la navigazione della vittima e registra un video dallo schermo se visita un sito pornografico. Obiettivo estorsione?

L’inventiva dei cyber-criminali, in alcuni casi, è davvero ammirevole. Pur di spremere qualche euro alle loro vittime sono infatti capaci di inventarsi qualsiasi tipo di truffa e attacco, modificando le loro strategie in base alle esigenze del momento.

Il caso del trojan **Varenyky**, individuato dai ricercatori di **ESET**, è la dimostrazione di questa straordinaria capacità di fiutare un nuovo “affare”, puntando a estorcere denaro agli sventurati che ne finiscono vittima.

Come spiegano i ricercatori in un report pubblicato sul blog della società di sicurezza, Varenyky è comparso in Francia e viene distribuito attraverso una campagna di spam via email che cerca di attirare le potenziali vittime con classiche tecniche di phishing.

Nel dettaglio, il messaggio in francese fa riferimento a una presunta fattura da 491,27 euro ed è scritto con una certa cura.

Il trojan viene installato quando la vittima apre il documento **Word** allegato, che richiede la solita attivazione delle macro mascherata, in questo caso, come un sistema di verifica per superare la protezione del documento e consentirne l'apertura.

Gli autori del malware, inoltre, hanno introdotto un piccolo accorgimento per renderne più difficile l'individuazione da parte dei sistemi di scansione automatica. **Prima di avviare l'installazione, infatti, i comandi macro verificano le impostazioni di Word per controllare che sia impostato per la lingua francese**.

Nel caso in cui la lingua sia un'altra, o sia impostata sulle versioni pensate per altri paesi francofoni come Belgio o Canada, l'esecuzione del codice si blocca.

Un ulteriore controllo, questa volta relativo al layout di tastiera, viene effettuato all’inizio dell’esecuzione del codice del trojan.

La logica è semplice: quando il file finisce su un computer impostato con un’altra lingua (per esempio quelli usati dalle società di sicurezza per analizzare i file intercettati su Internet) il documento appare innocuo.

Le funzionalità di Varenyky comprendono moduli classici, come il furto delle credenziali di accesso ai servizi Internet, ma anche uno strumento piuttosto originale. Il trojan, infatti, esegue un monitoraggio della navigazione su Internet.

Obiettivo: individuare il momento in cui il proprietario del computer si collega a un sito con materiale pornografico.

Quando questo avviene (il malware verifica una serie di parole chiave) Varenyky attiva un sistema di registrazione dello schermo attraverso **FFmpeg**, che lo stesso trojan scarica e avvia. **Il video viene poi inviato al server Command and Control gestito dai pirati informatici**.

L'obiettivo, anche se i ricercatori di ESET usano il condizionale, è probabilmente quello di utilizzare il video per ricattare la vittima, minacciando di rendere pubblico il video nel caso in cui non paghi un riscatto.

Insomma: si tratterebbe di una nuova versione della **truffa a luci rosse**, di cui abbiamo parlato ampiamente in passato e che sembra aver fruttato centinaia di migliaia di dollari ai suoi autori.

Nel caso della truffa a luci rosse, però, il ricatto si basava su un bluff. Con Varenyky le cose vanno decisamente peggio, visto che in questo caso gli estortori avrebbero veramente tra le mani un video compromettente.

Condividi l'articolo

Il 5G è agli esordi ma ci sono già problemi di sicurezza

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/09/varenyky-e-arrivato-il-trojan-a-luci-rosse/

”Sono il tuo vicino di numero”. Il gioco su WhatsApp che vìola la privacy

“Ciao, sono il tuo vicino di numero”. Se arriva anche a voi un messaggio con questo testo significa che siete stati coinvolti nel “gioco” dell’estate: inviare un messaggio, su **WhatsApp**, **SMS** o **iMessage**, al numero di telefono precedente o successivo al proprio cambiando l’ultima cifra e poi pubblicare la conversazione su **Twitter**. È l’ultima tendenza che arriva dagli Usa (con l’hashtag #numberneighbor) e si sta diffondendo anche in Italia con #vicinodinumero. Ma la condivisione sul social dello scambio di messaggi rischia di violare la privacy di chi è vittima del “gioco”. Infatti, seguendo il flusso di tweet sul tema si leggono integralmente le conversazioni e si vedono addirittura anche le foto delle persone inviate nella chat. Invece, quasi sempre non sono visibili i numeri di telefono.

La moda, che era già stata segnalata nel 2016 sempre negli Stati Uniti, è stata rilanciata nei giorni scorsi dal batterista americano **Ryan Lavallee** che ha pubblicato su Twitter la conversazione con il suo vicino di numero. Negli Usa, al gioco ha partecipato anche la squadra di baseball **Cleveland Indians**: ha pubblicato un simpatico scambio di messaggi con il proprio vicino di numero che tifa la squadra rivale.

https://www.key4biz.it/sono-il-tuo-vicino-di-numero-il-gioco-su-whatsapp-che-viola-la-privacy/268246/

iOS 13 privacy feature will force total overhaul for Facebook apps

Apple’s Craig Federighi unveils iOS 13 at WWDC 2019.

reader comments

104 with 73 posters participating

Share this story

Privacy has been a renewed focus with Apple’s next operating system update. One new feature in iOS 13 that seems centered on user privacy could have sweeping consequences for messaging and online call apps.

In iOS 13, Apple will not allow apps to run voice over Internet protocol (VoIP) in the background when the programs are not actively in use. Many apps that offer VoIP services currently run in the background, and they will need to be rewritten to adjust to Apple’s upcoming rules. The change is slated to roll out when iOS 13 is released in September. However, app developers will get a grace period, and they have until April 2020 to comply.

Apple has been putting privacy at the front and center of its business, especially as many tech companies make headlines for data breaches or misuse of personal information. iOS 13 will include multiple updates centered on giving users more control over how and when apps can get their information, such as one-

time location sharing and a “Sign in with Apple” system.

VoIP services ostensibly stay running in the background so they can connect calls quickly, but they also let those apps collect information about what users are doing on their devices. Restricting the programs that can simply be open at any time on its mobile hardware fits the narrative Apple is crafting about being a trusted place for customer privacy in an increasingly untrustworthy industry.

The move will force many apps to make some big changes. Possibly the most visible apps impacted by the update will be Facebook’s Messenger and WhatsApp programs. Both of those apps give users the option to make calls, and they run in the background of a smartphone so that they can quickly connect calls.

The Information first reported on the story, and a representative from Facebook said that the company is in talks with Apple about this development:

> *The changes to the upcoming iOS releases are not insignificant, but we are in conversations with Apple on how best to address. To be clear—we are using the PushKit VoIP API to deliver a world-class, private messaging experience, not for the purpose of collecting data.*

Facebook may not have data collection as the explicit purpose of its VoIP programs, but that doesn’t mean the social network isn’t doing so. Its track record for privacy issues is not good. Facebook incurred the scrutiny of the Federal Trade Commission, along with a $5 billion settlement and closer oversight, over charges surrounding misuse of user data. It also stored email-address lists and collected email passwords from its users this spring. And many people have anecdotal experience of seeing freakishly accurate or timely targeted ads when they use Facebook’s services.

This won’t be the first time Apple and Facebook lock horns over their approaches to privacy and customer protections. Apple took a drastic action against Facebook in January: Apple removed the social media giant’s certificate for its Enterprise Developer Program after it uncovered that Facebook was improperly using it to distribute apps that monitored user activity. And even that wasn’t Facebook’s first Apple infraction.

It’s unclear if Facebook’s reps think they can convince Apple to reverse course completely, or if they will be looking for a longer grace period to rework apps, or if they have a different end goal. A total 180 from Apple seems unlikely given its hawkish attitude toward privacy, but we’ll be watching closely to see if it cedes any additional ground to VoIP app developers.

https://arstechnica.com/?p=1547123

Capital One, UniCredit smentisce il data leak: ‘Nessuna violazione’

Dopo aver condotto un’indagine interna, **UniCredit** ha rivelato che non sussisterebbe alcuna prova del suo coinvolgimento nella violazione dei dati di **Capital One**. Lo ha dichiarato l’Istituto bancario in una nota interna indirizza ai dipendenti.

L’azienda ha infatti affermato di non aver trovato prove di violazione, sottolineando come i dati dei propri clienti non siano stati salvati sui server **Amazon** hackerati.

La violazione a Capital One

Il 30 luglio **Capital One**, holding bancaria con Sede in Virginia, ha dichiarato di aver subìto una data leak che ha coinvolto circa 100 milioni di persone negli Stati Uniti e 6 milioni in Canada.

Secondo la banca americana i criminali informatici sono riusciti a sfruttare una "*vulnerabilità di configurazione*" nella strutture informatiche dell'azienda rubando dati sensibili quali: nomi, indirizzi, numeri di telefono ed estratti conto.

L'azienda ha però precisato che gli hacker non sono arrivati ad avere accesso ai numeri di conto corrente collegati ai numeri di carte di credito.

UniCredit

UniCredit ieri ha dichiarato di aver avviato un'indagine sulla vicenda dopo che il nome della banca è stato citato in un blog come un possibile obiettivo della presunta hacker, **Paige A. Thompson,** una ex dipendente di Amazon.

Secondo Capital One, Thompson "*ha utilizzato le credenziali del firewall dell'applicazione Web per raggiungere il database del clienti della banca e di altre organizzazioni finanziarie*".

Non solo UniCredit, ma anche la **Ford** ha avviato indagini per accertare se i propri dati siano stati hackerati durante l'hackeraggio alla holding bancaria, ma la casa automobilistica americana al momento non ha ancora rilasciato dichiarazioni ufficiali.

https://www.key4biz.it/capital-one-unicredit-smentisce-il-data-leak-nessuna-violazione/267809/

Libra, Facebook: 'Troppe pressioni, a rischio il lancio della criptovaluta'

La valuta digitale che **Facebook** intende lanciare nel 2020 forse non avverrà mai. Perché? Perché l'azienda di **Mark Zukerberg** ha riconosciuto ciò che molti hanno detto: che le questioni normative potrebbero essere una barriera insormontabile al lancio del progetto.

Libra ha sollevato così tante preoccupazioni serie legate alla privacy e alla stabilità finanziaria che l'azienda di **Menlo Park,** a causa delle pressioni dalle autorità regolatorie e finanziarie, si vede costretta a rivedere i suoi piani per il lancio della criptovaluta.

In una chiara comunicazione dell'ultimo rapporto trimestrale dell'azienda alla **Securities and Exchange Commission** (SEC) degli Stati Uniti, l'azienda ha affermato: "*Libra ha attirato una significativa attenzione dei governi e delle autorità e ci attendiamo che questa attenzioni continui. A questo si aggiunge che l'accettazione da parte del mercato di tale valuta è soggetta a rischi significativi. Per questo non ci sono assicurazioni sul fatto che Libra e i prodotti associati* ***saranno resi disponibili in modo tempestivo, o del tutto****. Anzi, leggi e regolamenti possono ritardare o impedire il lancio della della criptovaluta".*

I problemi del progetto

Come ha affermato la società, Libra – che potrebbe potenzialmente portare all'adozione della criptovaluta per i 2 miliardi di utenti di Facebook – ha causato una sorta di tumulto nei circoli regolatori di tutto il mondo.

Banche centrali e Governi si sono messi in fila per chiedere maggiori informazioni sul progetto a causa dei timori che potrebbero costituire una minaccia la banca centrale e la stabilità finanziaria, oltre ai rischi per quanto riguarda il riciclaggio e le frodi.

Lo scorso 12 luglio, i ministri dell'Economia del G7 formarono una task force per esaminare i problemi relativi alle criptovalute, con un accento focalizzato sul progetto di Facebook. Dal Summit si è concluso che sarebbero stati necessari regolamenti di "livello più elevato" per poter comprendere la fattibilità del progetto.

Inoltre, i dubbi della società sulla fattibilità del suo progetto non sono nemmeno dovuti alla regolamentazione. La nota prosegue con un altro passo significativo riguardo la poca esperienza dell'azienda.

"Non abbiamo una significativa esperienza nelle valute digitali e nella tecnologia blockchain e questo potrebbe avere effetto sulla nostra capacità di sviluppare con successo e portare sul mercato questi prodotti e servizi" – conclude la nota -.

https://www.key4biz.it/libra-facebook-troppe-pressioni-a-rischio-il-lancio-della-criptovaluta/267274/

Privacy group asks court to reconsider FTC’s $5 billion Facebook deal

Enlarge / Thumbs down.
Getty Images | Ted Soqui

reader comments

37 with 26 posters participating

Share this story

A group of privacy and consumer organizations is asking a federal court to slow its roll on approving the Federal Trade Commission’s $5 billion settlement with Facebook, saying it doesn’t do nearly enough to protect individuals.

The Electronic Privacy Information Center (EPIC) filed the motion to intervene (PDF) with the US District Court in Washington, DC, on Friday, asking the court to let it and other privacy advocacy groups file comments in a “careful review of the fairness and adequacy” of the proposed settlement.

The agreement between Facebook and the FTC, as announced last week, includes a record-setting $5 billion fine and mandates changes to Facebook’s reporting structure and oversight for privacy-related matters.

As with any other settlement, the consent decree between

Facebook and the FTC is not final until after a judge approves. EPIC is specifically asking the court not to rubber-stamp it but instead to allow it and other privacy organizations to file briefs to the case and to schedule a hearing to review privacy-related issues.

The settlement is not “adequate, reasonable, or appropriate,” EPIC said in its filing. “Its scope goes far beyond the dispute in question, extinguishing all 26,000 pending consumer complaints” made about Facebook prior to June 2019.

“The proposed settlement is clearly not in the public interest, as it leaves consumer complaints unaddressed while still failing to ensure consumer privacy on Facebook,” the group continued. “This court has a mandate not to ‘stand by and approve any consent decree placed before it’ and ‘is not obliged to accept one that appears to make a mockery of judicial power’ like the consent decree proposed in this case.”

A collection of other advocacy groups, including Public Citizen, the Consumer Federation of America, the Center for Digital Democracy, the Campaign for a Commercial-Free Childhood, Color of Change, and Open Markets, all issued statements supporting the suit and expect to be involved with it going forward if the court allows.

“The public has a right to know what laws Facebook violated,” said Color of Change Senior Campaign Director Brandi Collins-Dexter. Corporations should face consequences for violating the public trust, not be given a rubber stamp to carry out business as usual.”

EPIC and the groups joining it are far from alone in criticizing the settlement. Other groups, such as Consumer Reports and the EFF, called for Congress to pass some kind of legislation protecting consumer privacy going forward.

https://arstechnica.com/?p=1542739

L’Australia vuole creare un organo di controllo per Facebook e Google

L’**Australian Competition and Consumer Commission**, l’autorità Antitrust dell’Australia, proporrà di istituire il primo ufficio al mondo di ‘controllo’ per i giganti del web.

Secondo l’ACCC questa nuova divisione di controllo per le piattaforme digitali avrebbe la responsabilità di “*sollevare il velo*” sui mercati pubblicitari e sugli algoritmi utilizzati in modo particolare da **Facebook** e **Google**.

Questi suggerimenti sono stati evidenziati nel report di 623 pagine pubblicato venerdì dal tesoriere australiano **Josh Frydenberg** e dal ministro delle comunicazioni **Paul Fletcher.**

> *News: Holistic, dynamic reforms needed to address dominance of digital platforms https://t.co/X24I1s6KO3*
>
> *— ACCC (@acccgovau) July 26, 2019*

Le raccomandazioni

Le 23 raccomandazioni – che abbracciano le leggi sulla concorrenza, la tutela dei consumatori, la regolamentazione dei media e la legge sulla privacy, riflettendo l’intersezione di questioni derivanti dalla crescita delle piattaforme digitali che il governo australiano deve ora decidere se applicare – costituirebbero uno dei regimi di applicazione più severi al mondo.

Secondo quanto afferma il rapporto, la divisione sarebbe in grado di tenere inchieste pubbliche per cinque anni e costringere le aziende tecnologiche a fornire informazioni pertinenti sul proprio funzionamento per capire meglio le dinamiche.

Le indagini esaminerebbero l'offerta di servizi pubblicitari, se vi sia sufficiente trasparenza sui prezzi applicati e se vi sia sufficiente concorrenza sul mercato.

Le piattaforme saranno inoltre tenute a sviluppare un codice di condotta per garantire che le aziende di notizie siano trattate in modo equo e trasparente e che ricevano tempestivamente notifiche sulle modifiche al ranking delle notizie. Il codice dovrebbe anche coprire i negoziati tra le piattaforme e le imprese di notizie sulla condivisione delle entrate derivanti dalla pubblicità, ha affermato l'ACCC.

Il resoconto dell'Australian Competition and Consumer Commission

Il rapporto afferma che 19,2 milioni di australiani hanno utilizzato Google ogni mese, 17,6 milioni hanno utilizzato **YouTube** (di proprietà di Google), 17,3 milioni di Facebook e 11,2 milioni di **Instagram** (di proprietà di Facebook). Per ogni 100 dollari spesi in pubblicità online, 47 dollari sono andati a Google, 24 a Facebook e 29 al resto.

L'ACCC ha inoltre raccomandato che le piattaforme digitali siano tenute ad attuare un codice di condotta per disciplinare il modo in cui hanno gestito i reclami sulla diffusione di informazioni inesatte, che sarebbero state registrate e applicate da un regolatore indipendente come l'Australian

Communications and Media Authority.

La legge sulla privacy dovrebbe essere aggiornata per offrire agli utenti un maggiore controllo sulle loro informazioni personali, la possibilità di spostare i dati da una società all'altra, di farli distruggere e di richiedere maggiori livelli di consenso da parte degli utenti prima che le informazioni personali vengano raccolte, rapporto raccomandato.

"*Non c'è altra scelta che istituire il giusto regime normativo e legislativo per proteggere la privacy del pubblico*", ha dichiarato Frydenberg durante la presentazione. "*Ciò che questo rapporto rileva è che così tanti dati personali vengono raccolti senza il consenso informato.*"

Facebook

Dopo la multa a Facebook da parte dell'FTC di 5 miliardi di dollari per lo scandalo di Cambridge Analytica, il report indica al governo australiano di attuare le raccomandazioni della Commissione di riforma della legge australiana e di introdurre un illecito legale per gravi violazioni della privacy.

Altre raccomandazioni includono il finanziamento dei contribuenti per il giornalismo locale e le organizzazioni di alfabetizzazione mediatica e la donazione a organizzazioni senza scopo di lucro impegnate nel giornalismo di interesse pubblico deducibile dalle tasse.

"*Siamo molto preoccupati del fatto che le attuali politiche sulla privacy offrano ai consumatori l'illusione del controllo, ma invece sono esenzioni quasi legali che offrono alle piattaforme digitali un ampio potere discrezionale su come possono utilizzare i dati dei consumatori*", ha affermato **Rod Sims**, presidente dell'ACCC.

Sims ha affermato, tuttavia, che il rapporto è "*l'inizio di un lungo viaggio*" e che il disinvestimento non potrebbe essere escluso in futuro.

Adesso le proposte della Accc saranno soggette a un processo di consultazioni pubbliche di 12 settimane, prima che il governo australiano prenda in mano il dossier.

Per approfondire

- Per scaricare il report "Digital Platforms Inquiry" dell'ACCC clicca qui.

L'Australia vuole creare un organo di controllo per Facebook e Google

---

FTC fines Facebook $5 billion, imposes new privacy oversight

Enlarge / The company can afford to shrug it off.

reader comments

7 with 7 posters participating

Share this story

The Federal Trade Commission today announced a long-rumored,

record-smashing $5 billion settlement with Facebook over allegations related to user privacy.

The fine is high, and the settlement demands more privacy oversight at the company. But what the deal does *not* do is find anyone, including CEO Mark Zuckerberg, personally responsible, nor does it mandate huge changes to the way Facebook collects data—only to the way it makes disclosures and honors user settings.

Facebook repeatedly "subverted users' privacy choices to serve its own business interests," the FTC said in the order (PDF). The company's actions violated a previous settlement requiring Facebook to adhere to certain privacy guidelines.

The commission voted 3-2 along party lines to support the settlement. The two commissioners who voted against adopting the settlement, Democrats Rebecca Kelly Slaughter and Rohit Chopra, said it went nowhere near far enough, leaving Facebook ample room to get up to mischief in the future.

What it's all about

The biggest set of charges in the settlement relate to Facebook allowing third-party app developers to access data about users' friends, without saying they were doing so—the heart of the Cambridge Analytica scandal.

"At least tens of millions of American users relied on Facebook's deceptive privacy settings and statements to restrict the sharing of their information," the complaint says, "When, in fact, third-party developers could access and collect their data through their friends' use of third-party developers' apps."

The settlement reflected several charges about how Facebook handled third-party app permissions for years, all brought to light by investigations that began in the wake of the

Cambridge Analytica revelations.

Additionally, the FTC said Facebook violated the earlier order by "misrepresenting" consumers' ability to opt out of facial recognition by using phone numbers provided for two-factor authentication for advertising purposes without notifying users and by storing user passwords without encryption.

The $5 billion penalty is equivalent to about 9% of Facebook's annual revenue, or 23% of its 2018 profit, FTC Chairman Joseph Simons said, adding that the fine is "unprecedented in global privacy enforcement" and "one of the largest civil penalties for any type of conduct in US history, alongside cases involving enormous environmental damage and massive financial fraud."

In addition to the blockbuster $5 billion deal, regulators also announced two separate, smaller settlements related to Facebook's privacy practices today. The first is a $100 million settlement between the FTC and Cambridge Analytica, the company of data scandal fame. The FTC charged Cambridge Analytica, along with developer Aleksandr Kogan and former CEO Alexander Nix, with deceiving customers by claiming they did not collect any personally identifiable data when, in fact, they did.

The US Securities and Exchange Commission also accused Facebook of deception, but of investors rather than of users. Facebook is paying $100 million to settle charges that, for two years, its disclosures "presented the risk of misuse of user data as merely hypothetical when Facebook knew that a third-party developer had actually misused Facebook user data," the SEC said.

The terms

In addition to the $5 billion fine, which goes straight to the US Treasury, the new order requires Facebook to establish and

adhere to a new governance structure for reviewing user privacy on its services, including Instagram and WhatsApp.

The company's board of directors must form an independent privacy committee, removing "unfettered control" of decisions affecting user privacy from CEO Mark Zuckerberg. Members of that privacy committee will be nominated by a separate independent nominating committee, and they can only be removed by a supermajority of the eight-member board.

The agreement also requires that committee to designate specific compliance officers who will be responsible for handling privacy compliance at Facebook. Only that committee can remove those compliance officers, the FTC noted, not Zuckerberg or other Facebook employees.

In addition to FTC monitoring, a third-party entity will also regularly review Facebook's data collection practices for the next 20 years. That assessor's findings "must be based on the assessor's independent fact-gathering, sampling, and testing, and must not rely primarily on assertions or attestations by Facebook management," the FTC said.

Both Zuckerberg and the compliance officers must submit quarterly and annual privacy certifications to the FTC, guaranteeing the company's compliance. Both civil and criminal penalties are possible if those certifications are found to be false.

The company must also agree to a litany of other requirements, including greater oversight of third-party apps, beefed up disclosures about facial recognition, the establishment of a new data security program, and more.

Facebook in a statement said the settlement would bring "rigorous new standards for protecting your privacy."

The agreement "will require a fundamental shift in the way we approach our work" and will "mark a sharper turn toward

privacy, on a different scale than anything we've done in the past," the company continued. "The accountability required by this agreement surpasses current US law and we hope will be a model for the industry."

Facebook's statement omits the fact that the US does not have a national privacy law.

Transparency not included

Slaughter said in her dissent (PDF) that the settlement "falls short" against the allegations in the case. "I don't think the terms in this order go far enough to change Facebook or ensure accountability," she said. "There are no substantive limitations on Facebook's data collection, use, and sharing. And there is no public transparency."

The record "more than justified initiating litigation against Facebook and Mr. Zuckerberg," Slaughter said. "When executives at large companies exercise control over decisions, including decisions to break the law, they should be held accountable the same way executives at smaller companies are."

Although going to court does carry the risk of losing your case, "even an adverse finding or a lackluster remedy can further the public good," she wrote. "Disappointing results help build the public case that there are deficits in the law that Congress must address."

Aside from the issue of suing Zuckerberg, Slaughter said, the $5 billion, while an objectively large sum of money, is nowhere near enough. "I regard the injury to the public and the institutions of our democracy to be quite substantial," she said. Facebook could and should easily pay much more, she said, since FTC orders, such as the 2011 one the company now stands accused of violating, clearly do not motivate it to behave better.

Chopra's dissent (PDF) voiced similar sentiments.

Nothing in the order gives Facebook any incentive to leave its lucrative behavioral advertising model behind, and so in the long run, nothing will change, Chopra said:

> *This thirst for data has led the company to harvest intimate, personal details about tens of millions of Americans on a scale and scope that are almost unimaginable. Facebook's data collection is both ongoing and increasing, as the company continues to add new means of surveillance that can be difficult to avoid. To facilitate further data acquisition, Facebook grants itself the right to surveil, own, and monetize users' private information by binding them to constantly evolving take-it- or-leave-it terms at sign-on.*

The $5 billion fine "makes for a good headline," he wrote, "but the terms and conditions, including blanket immunity for Facebook executives and no real restraints on Facebook's business model, do not fix the core problems that led to these violations."

A win for Facebook?

Technology expert Ashkan Soltani, who served as the FTC's chief technologist for a time during the Obama administration, said on Twitter that the settlement "was a *terrible* outcome for our leading privacy regulator and a very sweet deal for Facebook." He added that, "If this were a game of chess, Facebook just checkmated FTC, flipped the board so it couldn't be played again, and covered the whole thing up with a blanket."

Soltani is not alone in his assessment. Several lawmakers have already heaped scorn on the arrangement. "The FTC not only fell short, it fell on its face," Sen. Edward Markey (D-Mass.) said. "Facebook is getting away with some of the most

egregious corporate bad behavior in the age of the Internet," he added. "This outcome is an insult to consumers."

The frustration isn't limited to Democrats, either. "This is very disappointing," Sen. Josh Hawley (R-Mo.) said. "This settlement does nothing to change Facebook's creepy surveillance of its own users and the misuse of user data. It does nothing to hold executives accountable. It utterly fails to penalize Facebook in any effective way."

FTC Chairman Simons, for his part, pointed to the law as the major issue. For the second time in a week, he called on Congress to pass privacy legislation and give the FTC authority to enforce it.

"We are a law enforcement agency without the authority to promulgate general privacy regulations," Simons said. "Our authority in this case comes from a 100-year-old statute that was never intended to deal with privacy issues like the ones that we address today."

The commission only had two choices, he continued: "One, settle on excellent terms—or two, litigate for years and likely come away, even from a favorable court decision, with far less relief than we announced today. Would it have been nice to get more? To get $10 billion instead of $5 billion, for example? To get greater restrictions on how Facebook collects, uses, and shares data?"

Maybe so, Simons implied, but the agency "cannot impose such things by our own fiat."

https://arstechnica.com/?p=1540807

Facebook patteggia con la Ftc multa di 5 miliardi di dollari per lo scandalo Cambridge Analytica

Facebook ha patteggiato con la **Federal Trade Commission** (Ftc) la cifra record di 5 miliardi di dollari per chiudere la disputa sulle violazioni della privacy degli utenti Usa con lo scandalo Cambridge Analytica. L'annuncio è stato dato dall'Antitrust statunitense, che aveva cominciato ad indagare nel marzo del 2018 quando fu scoperto che la società Cambridge Analytica era venuta in possesso, illecitamente, dei dati di circa 87 milioni di utenti Facebook per scopi politici. La Ftc ha chiuso l'indagine con una sanzione di 5 miliardi di dollari patteggiata oggi dalla società guidata da **Mark Zuckerberg**.

La multa "*è la maggiore mai comminata a una compagnia per violazione della privacy dei consumatori e quasi venti volte più salata della multa più alta mai comminata per lo stesso motivo a livello mondiale*", si legge nella nota della Ftc, che ha imposto a Facebook anche una serie di nuove restrizioni sulla gestione della privacy degli utenti e di modifiche alla struttura aziendale. Zuckerberg non è più il responsabile della protezione dei dati degli utenti della piattaforma e la società deve ora dar vita a un comitato indipendente del consiglio di amministrazione per supervisionare le decisioni sulla privacy e richiedere a un "assesor" indipendente di terze parti di valutare l'efficacia del programma sulla privacy di Facebook.

Tra le restrizioni previste dall'accordo, siglato

dall'Antitrust Usa e Facebook, "*il fondatore e ceo di Facebook Mark Zuckerberg sarà tenuto a certificare, ogni trimestre, che la società è conforme alle nuove restrizioni sulla privacy e potrebbe essere soggetta a sanzioni civili e penali per false certificazioni*".

"*Nonostante le ripetute promesse ai miliardi di utenti mondiali Facebook ha danneggiato le scelte dei consumatori* – ha detto **Joe Simons**, presidente dell'Ftc – *l'ampiezza della multa da 5 miliardi e le indicazioni di condotta sono precedenza nella storia della Ftc e hanno l'obiettivo non solo di punire le future violazioni, ma, cosa più importante, cambiare l'intera cultura sulla privacy di Facebook per diminuire la possibilità' di nuove violazioni*".

https://www.key4biz.it/facebook-patteggia-con-la-ftc-multa-di-5-miliardi-di-dollari-per-lo-scandalo-cambridge-analytica/266646/

La Russia come gli USA: ecco i piani di spionaggio sul Web

Lug 22, 2019 Marco Schiaffino In evidenza, Leaks, News, Privacy, RSS 0

Un gruppo hacker ha violato i sistemi di un contractor dei servizi segreti russi. Tra i progetti un sistema

per de-anonimizzare il circuito Tor.

Non è ancora comparso nessun "**Edward Snowden** russo", ma a svelare i progetti di Mosca per il controllo di Internet è bastata l'azione di un gruppo hacker.

Protagonista dell'azione un gruppo chiamato **0v1ru$**, che ha preso di mira i server della **SyTech**. Si tratta di un'azienda russa che lavora per conto del **FSB** (l'ex **KGB**) portando avanti numerosi progetti collegati alla cyber-warfare e al controllo dei cittadini russi sul Web.

Dopo aver violato la Active Directory dell'azienda, gli hacker hanno sostituito la homepage con una Yoba-face (immagine molto in voga in Russia, che sta per "trolling") prima di pubblicare il contenuto dei documenti (**7.5 terabytes di dati**) ottenuti dai sistemi di SyTech.

Come racconta in un articolo la versione russa di BBC (il testo è in russo, consigliamo di usare la traduzione in inglese) il materiale è stato diffuso attraverso un account Twitter registrato il giorno stesso. Dai documenti emergono

alcuni progetti segreti su cui SyTech starebbe lavorando per conto del FSB.

- **Nautilus** –Raccolta di informazioni sugli utenti dei social network come Facebook, MySpace e LinkedIn.
- **Nautilus-S** – De-anonimizzazione del traffico su **Tor** (il circuito per la navigazione anonima – ndr) utilizzando dei server "governativi" all'interno del circuito.
- **Reward** – Penetrazione dei circuiti Peer-to Peer, come Torrent.
- **Mentor** – Monitoraggio e ricercar di email sui server delle società russe.
- **Hope** – Creazione di un "mappa" delle rete Internet russa e delle modalità di connessione alle reti delle altre nazioni.
- **Tax-3** – Creazione di una intranet completamente separate degli altri network per memorizzare al suo interno informazioni sensibili riguardanti figure di primo piano dell'amministrazione, giudici e amministratori locali.

Alcuni dei progetti, come **Hope**, appaiono essere collegati a obiettivi più volte dichiarati dallo stesso governo russo, come la messa a punto di una "Internet autosufficiente" che sia in grado di rimanere attiva anche in caso di isolamento dalla rete globale.

Altri ricordano molto da vicino "esperimenti" simili portati avanti dagli USA. **A partire, per esempio, dal tentativo di inquinare la rete Tor, vista anche da Washington come un "problema"**.

Nautilus-S, tra le altre cose, sembra che sia uno dei progetti che è stato effettivamente messo in pratica. Stando ai documenti diffusi sarebbe stato avviato nel 2012 e a confermarne l'efficacia c'è un documento del 2014 che tratta esattamente della scoperta di server Tor su territorio russo che avevano la funzione di de-anonimizzare le comunicazioni sul circuito.

Condividi l’articolo

SonicWall Cloud App Security: sicurezza nell’età del cloud

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/22/la-russia-come-gli-usa-ecco-i-piani-di-spionaggio-sul-web/