# “Pegasus”, lo spyware per smartphone. Come funziona e come ci si può proteggere?

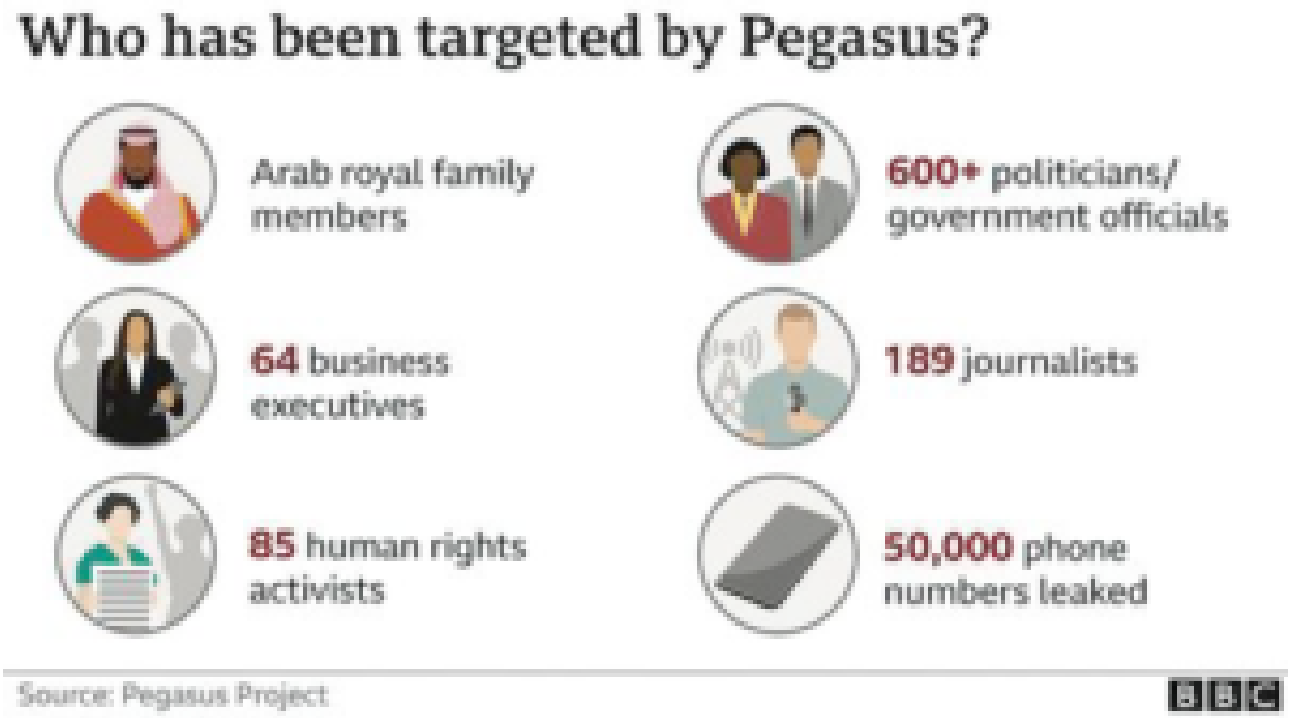
cybertrends.it/pegasus-lo-spyware-per-smartphone-come-funziona-e-come-ci-si-puo-proteggere/

Sandra Gagliardi 8 agosto 2022

Uno degli eventi più importanti nel mondo cibernetico nel 2021 è rappresentato dai risultati di un’indagine condotta dal Guardian e da altre 16 organizzazioni mediatiche, che ha rilevato che più di 30.000 attivisti per i diritti umani, giornalisti e avvocati in tutto il mondo potrebbero essere stati presi di mira con lo spyware Pegasus (Pegasus è un cosiddetto “software di sorveglianza legale” sviluppato dalla società israeliana NSO).

Il rapporto pubblicato nel luglio 2021, intitolato “Pegasus Project” (1), sostiene che il malware è stato distribuito su larga scala attraverso vari exploit, tra cui diversi zero-days che hanno preso di mira i sistemi iOS. Sulla base di analisi forensi di numerosi dispositivi mobili, il laboratorio di sicurezza di Amnesty International ha effettivamente scoperto che il software è stato ripetutamente utilizzato in modo improprio per scopi di sorveglianza.

L’elenco delle persone prese di mira comprende 14 leader mondiali e un gran numero di attivisti, difensori dei diritti umani, dissidenti ed esponenti dell’opposizione. Più tardi nello stesso mese, quando è stato pubblicato il rapporto del Guardian e di Amnesty, funzionari del governo israeliano hanno visitato gli uffici della NSO nell’ambito di un’indagine sulle accuse (2). Nell’ottobre 2021, la Corte Suprema indiana ha nominato un comitato tecnico per indagare sull’uso di Pegasus per spiare i cittadini (3). A novembre, Apple ha annunciato l’avvio di un’azione legale contro NSO Group per aver sviluppato un software che colpisce i suoi utenti con “malware e spyware”(4). Infine, nel dicembre 2021, Reuters ha pubblicato che i telefoni del Dipartimento di Stato americano, allertati da Apple, sono stati violati con il malware Pegasus di NSO (5).




Nel 2022, le rivelazioni sono continuate: il 2 maggio 2022, il governo spagnolo ha annunciato che il primo ministro Pedro Sánchez e il ministro della Difesa Margarita Robles erano entrambi monitorati da Pegasus (6). In seguito a queste rivelazioni, il governo spagnolo ha immediatamente licenziato il capo dei servizi segreti del Paese, Paz Esteban. Rilevare le tracce di Pegasus e di altre infezioni malware avanzate per dispositivi mobili è molto difficile ed è ulteriormente complicato dalle caratteristiche di sicurezza dei moderni sistemi operativi come iOS e Android. Secondo le nostre osservazioni, la loro analisi è resa ancora più difficile dal fatto che si tratta di distribuzioni di malware non persistenti, che non lasciano quasi alcuna traccia dopo il riavvio del dispositivo infetto.

Poiché molti strumenti forensi richiedono un jailbreak (completo, in questo caso, di intrusione consenziente) del dispositivo, il malware viene rimosso dalla memoria durante il riavvio, necessario per questa operazione. Fortunatamente, ad oggi, è possibile utilizzare diversi metodi per rilevare Pegasus e altri malware mobili. Ad esempio, il Mobile Verification Toolkit (MVT) di Amnesty International è gratuito (7), open source e consente a tecnici e investigatori di ispezionare i telefoni cellulari alla ricerca di segni di infezione. L'MVT è supportato da un elenco di IoC (indicatori di compromissione) compilato da casi di alto profilo di abuso dei diritti umani, reso disponibile anche da Amnesty International.

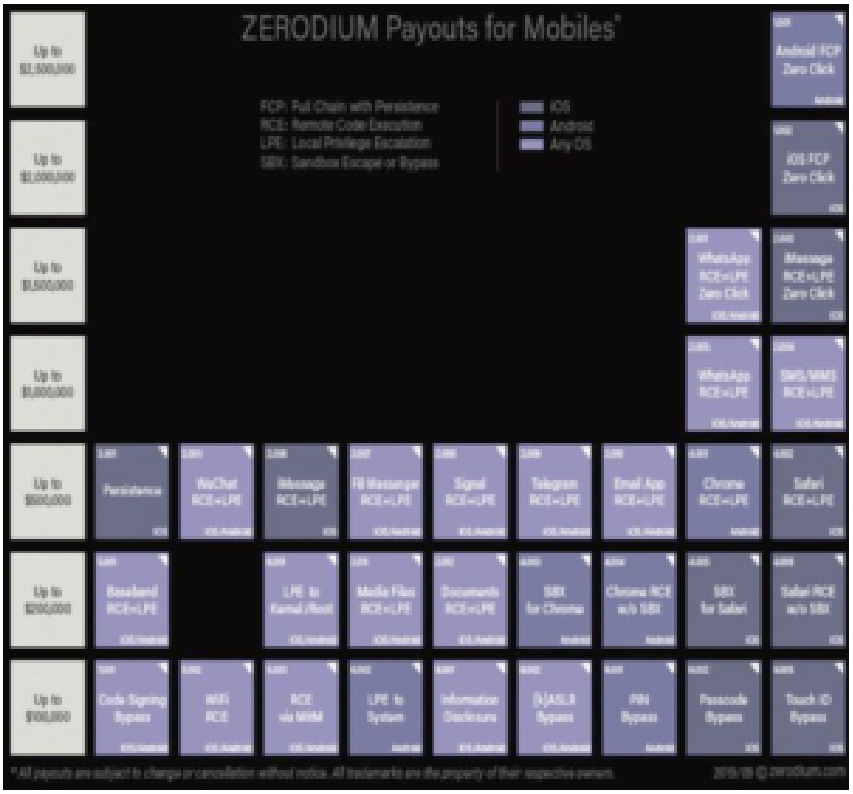
In questi tempi di incertezza, molti utenti preoccupati in tutto il mondo si chiedono come proteggere i propri dispositivi mobili da Pegasus e da altri strumenti e malware simili.

Allo stesso modo, i governi stanno cercando di valutare le proprie debolezze e di sviluppare strategie per identificare tali vulnerabilità, o almeno per evitare che si verifichino in futuro. In questo articolo esamineremo le più recenti tecniche di attacco utilizzate per distribuire


malware sui telefoni cellulari e come difendersi da esse, tenendo presente che un elenco di tecniche di difesa non è esaustivo. Inoltre, poiché gli aggressori cambiano il loro modus operandi, anche le tecniche di difesa esistenti devono essere adattate molto frequentemente.

**Come si fa a stare al sicuro dalle minacce informatiche mobili più sofisticate?**

Innanzitutto, va detto che Pegasus è un kit di strumenti dal prezzo relativamente alto. Il costo di un'implementazione completa può raggiungere facilmente i milioni di dollari. Allo stesso modo, altre minacce informatiche mobili possono essere distribuite attraverso exploit 0-click 0-day.




Questi sono estremamente costosi: ad esempio, Zerodium, una società di intermediazione di "exploit", richiede fino a 2,5 milioni di dollari per una catena di infezioni Android 0-click con persistenza avanzata:

Si può trarre subito una conclusione importante: lo spionaggio informatico sofisticato è un'attività che richiede molte risorse. Quando uno sponsor può permettersi di spendere milioni, o addirittura decine di milioni o centinaia di milioni di dollari USA in programmi offensivi, è altamente improbabile che un obiettivo possa evitare di essere infettato. In

pratica, più prosaicamente, non si tratta di “se si può essere infettati”, ma quando e come: è, infatti, solo una questione di tempo e del prima che voi siate infettati, grazie alle risorse corrispondenti ai vostri strumenti e al loro livello di sicurezza.

La buona notizia è che lo sviluppo di exploit e la guerra informatica offensiva sono spesso più un’arte che una scienza esatta. Gli exploit devono essere adattati a versioni specifiche del sistema operativo e dell’hardware e possono essere facilmente vanificati da nuovi sistemi operativi, nuove tecniche di mitigazione o persino da piccole cose come eventi casuali.

Da questo punto di vista, l’infezione e il bersaglio sono anche una questione di costi e difficoltà per gli aggressori. Sebbene non sia sempre possibile impedire lo sfruttamento e l’infezione di un dispositivo mobile, possiamo cercare di renderlo il più difficile possibile per gli aggressori.

Come lo facciamo nella pratica? Ecco una semplice lista di controllo:

**Su iOS:**


a) *Riavviare ogni giorno.*
Secondo le ricerche di Amnesty e CitizenLab, la catena di infezione di Pegasus si basa spesso su clic quotidiani senza persistenza, per cui un riavvio regolare ripulisce il dispositivo.

Se il dispositivo viene riavviato quotidianamente, gli aggressori dovranno reinfettarlo più volte. A lungo andare, questo aumenta le possibilità di rilevamento; potrebbe verificarsi un arresto anomalo o l’installazione di semplici app che rivelano un’infezione di natura stealth.
In realtà, non si tratta solo di teoria, ma di pratica: abbiamo analizzato un caso in cui un dispositivo mobile è stato preso di mira da un exploit 0-click (probabilmente FORCEDENTRY). Il proprietario del dispositivo lo ha riavviato regolarmente e lo ha fatto entro 24 ore dall’attacco. Gli aggressori hanno cercato di colpirlo più volte, ma alla fine hanno rinunciato dopo essere stati colpiti più volte durante i riavvii.

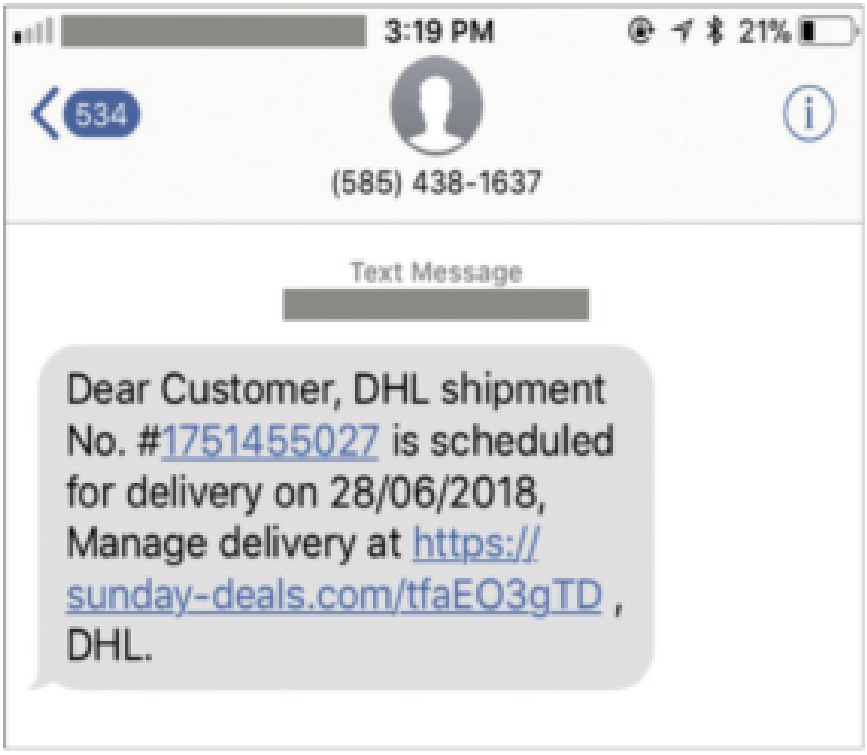
b) *Disattivare iMessage.*
iMessage è integrato in iOS ed è abilitato per impostazione predefinita, il che lo rende un interessante vettore di sfruttamento. Essendo abilitato per impostazione predefinita, è un meccanismo di consegna privilegiato per le stringhe da 0 clic.
Per molti anni gli exploit di iMessage sono stati molto richiesti, con guadagni significativi per le società di intermediazione di “exploit”. “Negli ultimi mesi abbiamo assistito a un aumento del numero di exploit per iOS, soprattutto per Safari e iMessage, sviluppati e venduti da hacker di tutto il mondo. Il mercato degli zero-day è talmente inondato di exploit per iOS che recentemente abbiamo iniziato a rifiutarne alcuni”, ha scritto il fondatore di Zerodium

Chaouki Bekrar nel 2019 a WIRED (8).
Ci rendiamo conto che questo potrebbe essere molto difficile per alcuni (in seguito), ma se Pegasus e altri malware APT mobili di fascia alta sono tra i modelli di minaccia che vi preoccupano, questo è un compromesso che vale la pena fare.

c) *Disattivare Facetime.*
Come sopra.

d) Mantenere aggiornato il dispositivo mobile; installare le ultime patch di iOS non appena disponibili.
Non tutti possono permettersi di utilizzare le vulnerabilità 0-day. In effetti, la maggior parte dei kit di exploit per iOS di cui siamo a conoscenza mira a vulnerabilità che sono già state corrette. Tuttavia, molte persone utilizzano telefoni più vecchi e rimandano gli aggiornamenti per vari motivi.
Se volete stare al passo con (alcuni) hacker sponsorizzati dallo Stato, aggiornate il vostro sistema operativo il prima possibile e imparate a non avere bisogno di emoji per installare le patch (9).

e) *Non cliccate mai sui link ricevuti nei messaggi SMS.*
È un consiglio semplice ma efficace. Non tutti i clienti di Pegasus possono permettersi di acquistare catene di 0-day da milioni di dollari, quindi si affidano a exploit da 1 clic.
Queste arrivano sotto forma di messaggio, a volte via SMS, ma anche tramite altri servizi di messaggistica o persino via e-mail. Se ricevete un SMS interessante (o un messaggio tramite qualsiasi altro servizio di chat) con un link, apritelo su un computer desktop, preferibilmente utilizzando TOR Browser o un sistema operativo sicuro non persistente come Tails.




*SMS contenente un link malevolo usato per colpire un attivista politico - credit: Citizenlab*

*f ) Navigare in Internet con un browser non nativo, come Firefox Focus, invece di Safari o Chrome.* Sebbene tutti i browser su iOS utilizzino praticamente lo stesso motore di ricerca, Webkit, alcuni exploit non funzionano bene (vedi il caso APT LightRighter / TwoSailJunk (10)) su alcuni browser alternativi:

```
detect_os()

return {
        mobile: (typeof window.orientation !== "undefined") || (navigator.userAgent.indexOf('IEMobile') !== -1),
        webkit: parseFloat(/AppleWebKit\/([\d.]+)/.exec(navigator.userAgent)[1]) || 0,
        safari: window.navigator.userAgent.indexOf('Safari') > -1,
        version: function()
        {
                var match = (navigator.appVersion).match(/OS (\d+)_(\d+)_?(\d+)?/);
        if(match) {
                var version = [
                    parseInt(match[1], 10),
                    parseInt(match[2], 10),
                    parseInt(match[3] || 0, 10)
                        ];
                    return parseFloat(version[0]+'.'+version[1]+version[2]);
            } else {
                return "unknown";
```

*Il sistema operativo LightRiver verifica la presenza di "Safari" nella stringa dell'agente utente.*

**Stringhe dell'agente utente su iOS da Chrome (sinistra) /Firefox (destra):**

| Stringa dell'agente utente di Chrome su iOS | Firefox Focus User Agent Channel su iOS |
|---|---|
| Mozilla/5.0 (iPhone; CPU iPhone OS 15_1 come Mac OS X) AppleWebKit/605.1.15 (KHTML, come Gecko) CriOS/96.0.4664.53 Mobile/15E148 Safari/604.1 | Mozilla/5.0 (iPhone; CPU iPhone OS 15_1 come Mac OS X) AppleWebKit/605.1.15 (KHTML, come Gecko) FxiOS/39 Mobile/15E148 Version/15.0 |

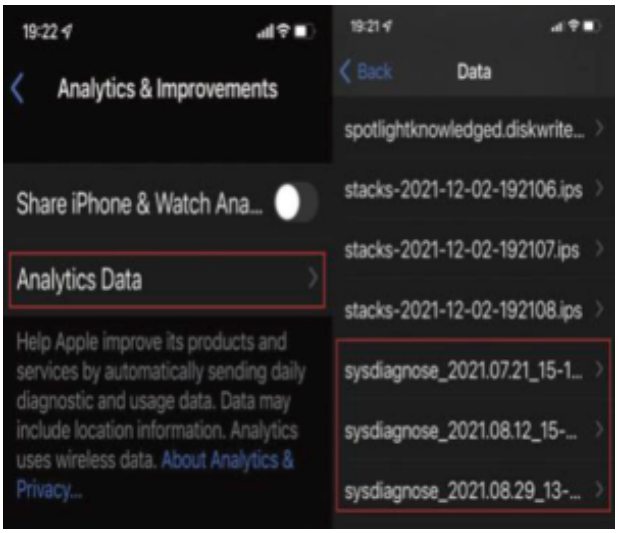
*g) Utilizzate sempre una VPN che mascheri il vostro indirizzo IP e il traffico dati.*
Alcuni exploit vengono trasmessi da attacchi MitM tramite l'operatore GSM, durante la navigazione di siti HTTP o tramite DNS hijacking. Utilizzando una VPN per mascherare il vostro indirizzo IP e il vostro traffico dati, è difficile per il vostro operatore di telefonia mobile individuarvi direttamente su Internet.
Complica inoltre il processo di targeting se gli aggressori hanno il controllo del flusso di dati, ad esempio durante il *roaming*.
Tenete presente che non tutte le VPN sono uguali e non tutte le VPN sono buone da usare. Senza individuare una VPN in particolare, ecco alcune cose da considerare quando si acquista un abbonamento VPN: Acquistare significa esattamente questo: niente VPN "gratuite".

- Cercate servizi che accettino pagamenti in criptovalute.
- Cercate servizi che accettino pagamenti in criptovalute.
- Cercate servizi che non richiedano di fornire informazioni di registrazione.
- Cercate di evitare le applicazioni VPN: utilizzate invece strumenti open source come WireGuard e OpenVPN e profili VPN.
- Evitate i nuovi servizi VPN e cercate quelli ben noti che esistono da tempo.

*h) Installare un'applicazione di sicurezza che controlli e avverta se il dispositivo è jailbroken.*
Frustrati dal fatto di essere presi a calci nel sedere più e più volte, gli aggressori finiranno per implementare un meccanismo di persistenza e "jailbreakare" il vostro dispositivo (accedere illegalmente a tutti i suoi contenuti). In questo caso le possibilità di catturare i malintenzionati si decuplicano e possiamo sfruttare il fatto che il dispositivo è stato jailbroken.

*i) Eseguire il backup di iTunes una volta al mese.*
Ciò consente di diagnosticare e individuare le infezioni in un secondo momento, utilizzando il meraviglioso pacchetto MVT di Amnesty.

*j) Attivare spesso i sysdiag e salvarli in backup esterni.*
Gli strumenti forensi possono aiutarvi a determinare in seguito se siete stati presi di mira. L'attivazione di un *sysdiag* (un'applicazione che consente una diagnosi completa del sistema e dei contenuti) dipende dal modello di telefono.
Ad esempio, su alcuni iPhone è sufficiente premere contemporaneamente i tasti VOL Su +




Giù + Accensione. È possibile che si debba giocare più volte con questi tasti finché il telefono non emette un segnale acustico. Una volta creato, il *sysdiag* apparirà nella diagnostica nella sezione “dati analitici”.

**2. Su Android**

*a) Riavviare ogni giorno*.
La persistenza sulle ultime versioni di Android è difficile, molti APT e fornitori di exploit evitano la persistenza!

b) *Mantenere il telefono aggiornato; installare le ultime patch.*

c) *Non cliccate mai sui link ricevuti nei messaggi SMS.*

d) *Navigare in Internet con un altro browser come Firefox Focus invece di Chrome.*

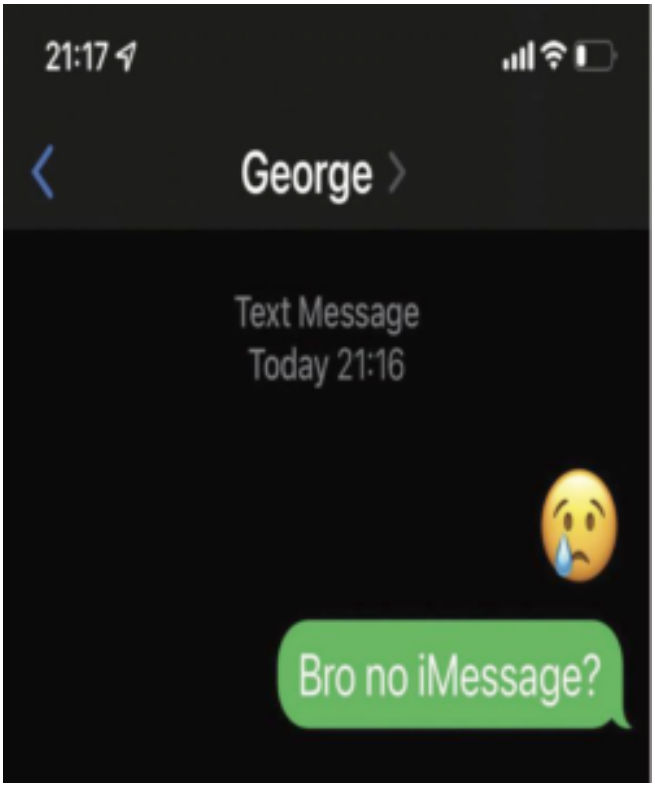
e) *Utilizzate sempre una VPN che mascheri il vostro indirizzo IT e il traffico dati.*
Alcuni exploit si diffondono tramite attacchi MitM agli operatori GSM, durante la navigazione di siti HTTP o tramite DNS hijacking.

f ) *Installare una suite di sicurezza che esegua la scansione del malware e controlli e avvisi se il dispositivo è jailbroken.*
A un livello più sofisticato, verificate sempre il traffico di rete utilizzando gli IOC dal vivo. Una buona configurazione potrebbe includere una VPN Wireguard sempre attiva verso un server sotto il vostro controllo, che utilizza pihole per filtrare le cose negative e registra tutto il traffico per una successiva ispezione (11).

**Una partita a punteggio zero?**

Ryan Naraine, un noto commentatore di sicurezza, ha dichiarato: *“iMessage e FaceTime – questi sono i motivi per cui la gente usa gli iPhone!*“ E ha ragione: iMessage e FaceTime sono due delle migliori aggiunte che Apple abbia fatto al suo ecosistema.

Fortunatamente, Apple ha migliorato notevolmente la *sandbox* di sicurezza che protegge iMessage con BlastDoor in iOS 14 (12). Tuttavia, l’exploit FORCEDENTRY utilizzato da NSO per distribuire Pegasus ha aggirato BlastDoor e, naturalmente, nessuna funzione di sicurezza è mai a prova di hacker al 100% (13).




BlastDoor in iOS 14 (12). Tuttavia, l'exploit FORCEDENTRY utilizzato da NSO per distribuire Pegasus ha aggirato BlastDoor e, naturalmente, nessuna funzione di sicurezza è mai a prova di hacker al 100% (13).

**Allora, cosa c'è di meglio in entrambi i mondi, vi chiederete?**

Alcune persone, me compreso, hanno più telefoni: uno con iMessage disattivato e un iPhone "*honeypot*" con iMessage attivato. Entrambi sono ovviamente associati allo stesso ID Apple e allo stesso numero di telefono. Se qualcuno decide di prendermi di mira in questo modo, è probabile che finisca nel telefono *honeypot*.

**Non tacete se siete osservati…**

Naturalmente, è possibile seguire alla lettera queste raccomandazioni ed essere comunque infettati. Purtroppo, questa è la realtà in cui viviamo oggi. Quando qualcuno ci dice di essere stato preso di mira da uno spyware mobile, gli diciamo di riflettere su queste domande:

- Chi vi ha preso di mira e perché?
- Cercate di capire cosa vi ha portato all'attenzione dei grandi.
- Potete evitarlo in futuro comportandovi in modo più discreto?
- Può parlarne?

Questo ha finito per far crollare molte società di sorveglianza, grazie alla cattiva pubblicità che tali casi hanno creato per loro, come quando molti reporter e giornalisti riportano gli abusi e smascherano le bugie e i misfatti generati da un operatore del settore.
Se siete stati presi di mira, cercate di trovare un giornalista e raccontate la vostra storia.

**Cambiare il dispositivo**

Se si utilizzava iOS, provare a passare ad Android per un po'. Se eravate su Android, passate a iOS. Questo può confondere gli aggressori per un po'; ad esempio, è noto che alcuni attori delle minacce acquistano sistemi operativi che funzionano solo su una determinata marca di telefono e di sistema operativo.

Acquistare un dispositivo secondario, preferibilmente con GrapheneOS, per comunicazioni sicure. Utilizzatelo con una carta prepagata o collegatevi solo tramite Wifi e TOR in modalità aereo.

Evitate i messaggi in cui dovete fornire il vostro numero di telefono ai vostri contatti. Una volta che un aggressore è in possesso del vostro numero di telefono, può facilmente prendervi di mira attraverso molti messenger diversi: iMessage, WhatsApp, Signal, Telegram, poiché sono tutti collegati al vostro numero di telefono.

Un'interessante novità è Session, che instrada automaticamente i messaggi attraverso una rete simile a Onion e non dipende dai numeri di telefono.

Cercate di entrare in contatto con un ricercatore di sicurezza della vostra zona e discutete costantemente delle migliori pratiche. Condividete con loro dati, messaggi sospetti o accessi non appena ritenete che ci sia qualcosa di strano.

La sicurezza non è mai un'unica soluzione istantanea che offra una garanzia al 100%; consideratela come un fiume, dove dovete adattare la vostra navigazione alla velocità, alle correnti e agli ostacoli.

Alla fine di tutto questo, vorrei lasciarvi con un pensiero. Se siete presi di mira da attori al servizio di Stati nazionali, significa che siete importanti.

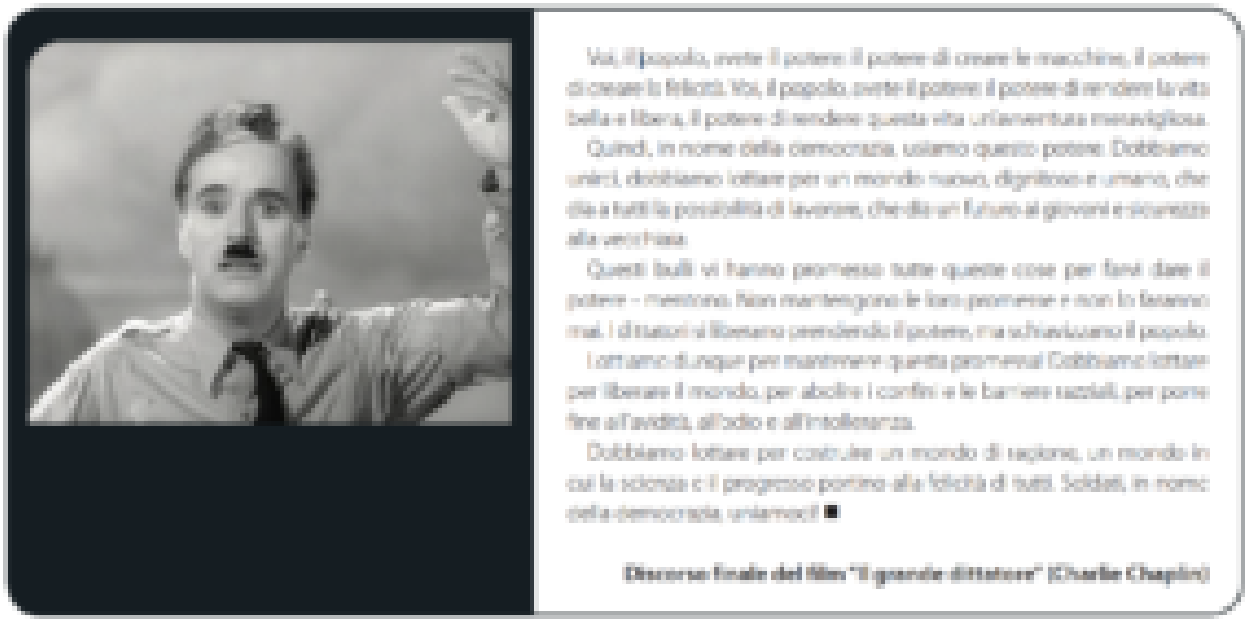
Ricordate: è bello essere importanti, ma è più importante essere gentili.

Da soli siamo deboli, insieme siamo forti.

Il mondo può essere distrutto, ma credo che stiamo vivendo un momento in cui possiamo ancora fare la differenza.

Secondo un rapporto del Committee to Protect Journalists (CPJ), nel 2021 sono stati imprigionati 293 giornalisti, il numero più alto mai registrato dal CPJ da quando ha iniziato a registrarlo nel 1992 (14).

Sta a noi dare forma a quello che sarà il mondo per noi tra 10 anni, per i nostri figli e per i figli dei nostri figli.



Voi, il popolo, avete il potere: il potere di creare le macchine, il potere di creare la felicità. Voi, il popolo, avete il potere di rendere la vita bella e libera, il potere di rendere questa vita un'avventura meravigliosa.

Quindi, in nome della democrazia, usiamo questo potere. Dobbiamo unirci, dobbiamo lottare per un mondo nuovo, dignitoso e umano, che dia a tutti la possibilità di lavorare, che dia un futuro ai giovani e sicurezza alla vecchiaia.

Questi bruti vi hanno promesso tutte queste cose per farvi dare il potere – mentono. Non mantengono le loro promesse e non lo faranno mai. I dittatori si liberano prendendo il potere, ma schiavizzano il popolo.

Lottiamo dunque per mantenere questa promessa! Combattiamo per liberare il mondo, per abolire i confini e le barriere razziali, per porre fine all'avidità, all'odio e all'intolleranza.

Dobbiamo lottare per costruire un mondo di ragione, un mondo in cui la scienza e il progresso portino alla felicità di tutti. Soldati, in nome della democrazia, uniamoci! ■

**Discorso finale del film "Il grande dittatore" (Charlie Chaplin)**

**Autore: Costin G. Raiu**

**Riferimenti**


*(1) https://www.amnesty.org/en/latest/news/2021/07/ the-pegasus-project/*
*(2) https://www.theguardian.com/news/2021/jul/29/ israeli-authorities-inspect-nso-group-offices-afterpegasus- revelations*
*(3) https://www.theregister.com/2021/10/29/india_ nso_pegasus_probe/*
*(4) https://www.theguardian.com/technology/2021/ nov/23/apple-sues-israeli-cyber-firm-nso-group*
(5) https://www.reuters.com/technology/exclusiveus- state-department-phones-hacked-with-israelicompany- spyware-sources-2021-12-03/
*(6) https://www.theguardian.com/world/2022/may/02/ spain-prime-minister-pedro-sanchez-phone-pegasusspyware*
*(7) https://github.com/mvt-project/mvt*
*(8) https://www.wired.com/story/android-zero-daymore- than-ios-zerodium/*
*(9) https://twitter.com/ryanaraine/ status/1324445133668974592*
*(10) https://securelist.com/ios-exploit-chain-deploylightspy- malware/96407/*
*(11) https://pi-hole.net*
*(12) https://googleprojectzero.blogspot.com/2021/01/ a-look-at-imessage-in-ios-14.html*
*(13) https://citizenlab.ca/2021/09/forcedentry-nsogroup- imessage-zero-click-exploit-captured-in-thewild/*
*(14) https://edition.cnn.com/2021/12/09/media/ journalists-imprisoned-cpj-census/index.html*