Gli Spyware: cosa sono e come difendersi

Una storia molto istruttiva: “The Million Dollar Dissident”

Per introdurre gli spyware e per comprenderne meglio l’importanza e la pericolosità, cominciamo raccontando una vicenda accaduta nel 2016: l’incredibile storia di Ahmed Mansoor, il “dissidente da 1 milione di dollari”, preso di mira dai software spia di tre diverse società.

Ahmed Mansoor è un ingegnere e blogger degli Emirati Arabi Uniti, noto difensore dei diritti umani, critico verso le politiche del governo degli Emirati. Per questo è stato perseguitato dal suo paese e arrestato per alcuni mesi nel 2011, malgrado avesse ricevuto da Amnesty International un premio come difensore dei diritti umani.



Il 10 e 11 agosto 2016 Mansoor riceve sul suo iPhone 6 due SMS (vedi figura) che promettono rivelazioni sulle torture nelle carceri degli Emirati. Gli SMS contengono un link. Anche stavolta si punta sul *social engineering* per convincere la vittima ad abboccare al phishing. Ma Mansoor, sapendo di essere nel mirino, si insospettisce e invia gli SMS a Citizen Lab[1], un laboratorio di cybersecurity dell’università di Toronto. Qui i messaggi vengono analizzati – in collaborazione con un’altra società di cybersicurezza, Lookout Security[2] – scoprendo che il link avrebbe attivato “Pegasus”: un micidiale malware per iOS che sfruttava tre gravi vulnerabilità zero-day (Trident iOS Exploit Chain).

I ricercatori hanno quindi avvisato Apple, che si è mossa

velocemente e ha chiuso le tre vulnerabilità con un importante e urgente aggiornamento di sicurezza iOS 9.3.5, rilasciato a fine agosto 2016. Vulnerabilità come queste sul mercato degli attacchi informatici erano valutate intorno a 1÷1,5 milioni di dollari.

Il malware Pegasus (realizzato dagli israeliani di NSO Group, che lo commercializza a Stati e polizie a prezzi di centinaia di migliaia di dollari) era uno **SPYWARE**: un software malevolo, in grado di violare un iPhone da remoto, senza che su questo fosse stato fatto precedentemente un *jailbreak*. Lo scopo dello spyware è sorvegliare l'attività della vittima, dalle telefonate, a WhatsApp e SMS, alle chat, dall'uso silente del microfono e della videocamera del dispositivo alla sua geolocalizzazione.

Il coinvolgimento di NSO Group che venderebbe solo a Stati e il tipo di vittima fanno concludere ai ricercatori di Citizen Lab che dietro l'azione ci possa essere il governo degli Emirati Arabi Uniti.

Anche perché Mansoor aveva già subito in precedenza altri due attacchi analoghi, portati da società simili a NSO Group: nel 2011 da FinFisher e nel 2012 dall'italiana Hacking Team.

Lo spyware italiano: il caso Exodus

Se la vicenda di Mansoor rappresenta un caso di spyware mirato, di alto livello e con finalità politiche, dobbiamo essere consapevoli che gli spyware possono colpire anche le persone comuni.

Nello scorso mese di aprile è apparsa la notizia di circa 25 applicazioni[3] presenti nel Play Store di Google (per Android) infettate da uno spyware chiamato "Exodus", che sarebbe finito negli smartphone di diverse centinaia di cittadini italiani, forse un migliaio, che non avevano nulla a che fare con inchieste e procedimenti penali.

Nel tentativo di indurre le potenziali vittime a installarle con l'inganno, le applicazioni contenenti lo spyware erano progettate per assomigliare a innocue app per ricevere promozioni e offerte di marketing da operatori telefonici italiani, o per migliorare le performance del dispositivo.

Le applicazioni sarebbero state sviluppate da una società italiana chiamata eSurv, di Catanzaro, che opera principalmente nel settore della videosorveglianza e che sembra essere fornitrice di questi prodotti anche alla Polizia di Stato italiana.

La scoperta dello spyware è stata fatta dai ricercatori di Security Without Borders[4], un'organizzazione non-profit che investiga sulle minacce contro i dissidenti e attivisti per i diritti umani, e dall'azienda di sicurezza ESET.

Questi ricercatori hanno scoperto che il malware Exodus scaricava un file ZIP per installare il vero malware, in grado di hackerare lo smartphone e di rubarne i dati.

Ottenendo in questo modo il controllo del dispositivo, il malware ha accesso ai dati più sensibili presenti sul telefono infettato, quali le chiamate telefoniche, la cronologia dei browser, le informazioni del calendario, la geolocalizzazione, i log di Facebook Messenger, le chat di WhatsApp e i messaggi. Inoltre era anche in grado di fare eseguire dei comandi al telefono spiato grazie a una shell e a una porta dati che veniva aperta (una cosiddetta "backdoor").

Non è ancora chiaro quali siano i motivi per i quali queste applicazioni infette siano state diffuse tra comuni cittadini: la Procura di Napoli ha avviato un'indagine "finalizzata all'accertamento di gravi reati collegati alla gestione di software utilizzati per l'intercettazione di comunicazioni telematiche con captatore informatico". Nell'ambito dell'inchiesta la Procura di Napoli ha iscritto nel registro degli indagati quattro persone. Il Gip ha adottato lo scorso

20 febbraio il decreto di sequestro preventivo dell'infrastruttura delle aziende di E-Surv, ideatrice delle applicazioni, e Stm, che si occupava della commercializzazione.

Cosa ci insegnano queste due vicende, diverse eppure con alcune similitudini?

- Gli Spyware possono essere molto pericolosi, anche se in genere – ma non solo – colpiscono obbiettivi mirati;
- qualsiasi smartphone, anche un iPhone (nonostante sia ritenuto più sicuro) può essere vulnerabile, soprattutto se non viene mantenuto aggiornato;
- da un messaggio (SMS o WhatsApp che sia) possono arrivare minacce importanti;
- questi malware possono essere introdotti anche attraverso applicazioni che nascondono al loro interno lo spyware;
- come sempre il fattore umano fa la differenza: se Mansoor fosse stato meno attento (o meno consapevole dei rischi) l'attacco avrebbe avuto successo e per lui sarebbero stati grossi guai.

Cosa sono gli Spyware

Oggi i nostri smartphone contengono tante informazioni e vengono usati in modo continuo, quindi per il cybercrime (ma non solo!) può essere più utile spiare il dispositivo piuttosto che rubarlo. Questo può essere realizzato utilizzando un particolare tipo di malware che, come abbiamo spiegato, viene definito "Spyware".

Lo spyware è un'applicazione di monitoraggio (spionaggio) che viene introdotta in uno smartphone all'insaputa del proprietario. Può essere installata:

1) **con accesso diretto al dispositivo**. Per questo motivo è importante fare sempre attenzione a non lasciare lo smartphone

incustodito senza un codice di blocco. Vedremo successivamente come questi software malevoli siano facilmente reperibili sul mercato e anche una persona non particolarmente esperta potrebbe installarlo nello smartphone di un altro (magari un collega o un familiare…);

2) **da remoto**: le tecniche per riuscire a installare l'applicazione (con tutti i permessi necessari) passano ancora una volta attraverso il phishing, il *social engineering* e la navigazione Web (le modalità d'intrusione sono sempre le stesse). Questo è il caso accaduto ad Ahmed Mansoor. Oppure possono essere nascosti all'interno di applicazioni o giochi gratuiti, come nella citata vicenda di Exodus.

Una volta installato, lo spyware può inviare all'esterno i dati contenuti nello smartphone – telefonate, messaggi, e-mail, foto – e attivare funzioni all'insaputa dell'utente, come fotocamera e microfono.

Il mondo degli spyware è molto variegato: si va da quelli "artigianali" reperibili nel web a poco prezzo, fino a prodotti altamente sofisticati, realizzati da aziende specializzate (come NSO Group), che li vendono alle polizie e agli enti governativi.

Un rapporto pubblicato dal già citato Citizen Lab ha rivelato che lo spyware Pegasus di NSO Group è stato utilizzato contro obiettivi in 45 Paesi del mondo.

Pegasus (utilizzato contro Mansoor) è – come detto – un malware di spionaggio che può infettare sia gli iPhone che i dispositivi Android ed è – o dovrebbe essere – venduto esclusivamente ai governi e alle forze dell'ordine.

Citizen Lab ha rilevato che lo spyware NSO è stato utilizzato in attacchi contro 175 obiettivi in tutto il mondo. Questi attacchi si sono realizzati soprattutto contro individui in Qatar o in Arabia Saudita, dove il software di sorveglianza israeliano sta diventando molto popolare, con evidenti e serie

implicazioni sui diritti umani delle persone. Si sospetta che fosse presente anche nell'iPhone del giornalista saudita Jamal Khashoggi, ucciso lo scorso ottobre nel consolato dell'Arabia Saudita a Istanbul.

Quando questi programmi vengono impiegati dalle polizie a scopo di spionaggio, si parla di "**captatori informatici**", utilizzati a fine di indagine per l'intercettazione di comunicazioni o conversazioni in dispositivi elettronici portatili.

Questi strumenti, per quanto utili a fini investigativi, rischiano, se utilizzati in assenza delle necessarie garanzie, di determinare inaccettabili violazioni della libertà dei cittadini, fino ad arrivare a scenari da "sorveglianza di massa" e, conseguentemente, a potenziali indebite pratiche di spionaggio.

Su questo delicato tema è stato approvato a fine 2017 un decreto che tratta le disposizioni in materia di intercettazioni (D.Lgs. 29 dicembre 2017, n.216[3], c.d. Decreto Orlando, dal nome dell'allora ministro della Giustizia) allo scopo di regolamentarne l'utilizzo e impedire gli abusi.

Il governo Conte ha successivamente disposto la proroga, dal 26 luglio 2018 al 31 marzo 2019, dell'entrata in vigore del D.lgs n. 216.

Non esistono solo prodotti di alto livello, come quelli venduti (a centinaia di migliaia di dollari!) da NSO Group. Come ho scritto, si possono trovare nel web degli spyware meno raffinati e a buon mercato. Non occorre cercarli nel Darkweb, perché sono distribuiti come applicazioni "legali" (0 che vorrebbero far credere di esserlo).

Molte di queste applicazioni vengono vendute infatti con lo scopo ufficiale e dichiarato di "controllare lo smartphone dei propri figli". In realtà si tratta di programmi la cui

installazione nel dispositivo di un terzo (senza la sua autorizzazione) rappresenta un vero e proprio reato.

Ne cito qui alcuni (senza riportare i link dove trovarli), che tutti possono acquistare e utilizzare per spiare qualcun altro (la moglie, il marito, il collega, ecc.):

SpyFone: commercializzato come "the world's number one parental monitoring software". L'azienda californiana che lo vende dichiara che ci vogliono appena 15 minuti per installare lo spyware sul dispositivo di destinazione e non vi è alcuna indicazione, per coloro che vengono spiati, che "qualcosa non vada" nei loro telefoni. Spyfone è in grado di monitorare l'attività degli smartphone, compresi i messaggi SMS inviati, registrare le chiamate e le informazioni provenienti da applicazioni come Skype e Whatsapp. Alcuni ricercatori hanno scoperto che SpyFone, oltre a compiere un'attività illegale, lascia i dati e le registrazioni esposte online, a causa di errori di configurazione dell'applicazione e delle API.

mSpy: è uno dei prodotti più noti, per iPhone e Android. Anche in questo caso il disclaimer dell'applicazione recita: "mSpy è progettato per monitorare i vostri figli, dipendenti o altri su uno smartphone o un dispositivo mobile di vostra proprietà o che avete il consenso a monitorare. L'utente è tenuto a notificare agli utenti del dispositivo che sono stati monitorati". Ma anche per mSpy le finalità reali sono ben altre e ovviamente illegali. L'accesso fisico diretto al dispositivo è necessario per installare mSpy (in circa 20 minuti). Ma – come successo per SpyFone – anche i dati spiati da mSpy sono stati violati ed esposti al pubblico dominio.

La violazione è stata segnalata dall'esperto di cyber sicurezza Brian Krebs che ha scoperto milioni di record sensibili pubblicati online, "tra cui password, registri delle chiamate, messaggi di testo, contatti, note e dati di localizzazione raccolti in segreto da telefoni che eseguono lo spyware".

Altri spyware facilmente reperibili in rete e di dubbia reputazione sono: Retina-X, FlexiSpy, Mobistealth, Spy Master Pro, SpyHuma, TheTruthSpy, Family Orbit, Copy9, Xnore.

Sembra incredibile, ma quasi tutte queste aziende che promettono di fornire servizi per i genitori per mantenere i figli al sicuro, monitorare i dipendenti, o spiare i coniugi, sono state violate negli ultimi due anni o hanno lasciato i dati esposti online.

Un motivo in più per non avere la tentazione di utilizzarle… oltre ai reati nei quali si incorrerebbe.

I sintomi degli Spyware

Non è facile capire se uno smartphone sia stato infettato da uno spyware.

Per i prodotti più sofisticati (come quelli realizzati da NSO Group), potrebbe non bastare neppure il reset del telefono alle condizioni di fabbrica, perché sono progettati per non essere visibili sullo smartphone della vittima e – nei casi più evoluti – per annidarsi nel Bootloader (il software che, all'accensione del dispositivo, ha l'incarico di caricare il sistema operativo installato).

Quelli meno evoluti (precedentemente elencati), pur riuscendo a non essere visibili, possono in genere essere eliminati con un reset del dispositivo. In altri casi – se si sospetta uno spyware – potrebbe essere necessario far esaminare il dispositivo da aziende specializzate, ma in questa eventualità i costi sono paragonabili a quelli per acquistare un nuovo smartphone…

Comunque l'esistenza dello spyware può essere quantomeno sospettata in presenza di sintomi quali:

- **riduzione della durata della batteria**: lo spyware è sempre attivo e consuma batteria anche se noi non stiamo

usando il telefono;
- **aumento anomalo del traffico dati**: lo spyware deve inviare all'esterno i dati raccolti;
- conseguente **aumento dei costi** non motivato;
- **prestazioni rallentate** e più in generale comportamento anomalo del cellulare.

Le buone regole difendersi dagli spyware sui dispositivi *mobile*

Come detto gli spyware vengono sempre utilizzati contro obbiettivi mirati: un avversario politico, ma anche un concorrente, un collega o – molto spesso – un coniuge.

Riassumiamo qui le "best practices" per difendersi dagli spyware, che come sempre riguardano il fattore umano (che è più che mai l'anello debole nella catena della sicurezza):

1. **installare applicazioni scaricate solo da fonti attendibili**, quali Google Play Store (anche se il controllo su questo store si è rivelato spesso debole), Apple App Store. Evitare (per Android) le applicazioni provenienti da repository di dubbia reputazione. Controllare feedback e recensioni degli utenti. Non fidarsi di link presenti in e-mail o sms che ci consigliano di installare un'applicazione;
2. **non cliccare su link** o allegati in e-mail o messaggi testuali (il caso di Ahmed Mansoor insegna);
3. mantenere il **sistema operativo sempre aggiornato**. Gli aggiornamenti sono finalizzati a risolvere le vulnerabilità presenti nel sistema operativo: uno smartphone aggiornato risulterà quindi meno attaccabile dai malware;
4. proteggere i dispositivi con una password forte. Impostare una password sicura (consiglio che non sia di sole quattro cifre numeriche, ma alfanumerica e di almeno otto caratteri) è diventata una necessita̗, per

evitare che qualcuno possa accedere al nostro smartphone, spiarlo e soprattutto installarvi un'applicazione malevola. Purtroppo, ancora oggi molte persone – per pigrizia e disattenzione – non impostano una password di blocco, sebbene l'utilizzo dei sistemi biometrici (touch-ID, Face-ID) renda questa opzione estremamente comoda: la password di sblocco dovrà essere digitata solo raramente, per esempio all'accensione dello smartphone.

Bibliografia

Giorgio Sbaraglia, *"Cybersecurity kit di sopravvivenza. Il web è un luogo pericoloso. Dobbiamo difenderci!"*, GoWare, 2018.

Note

[1] https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

[2] https://blog.lookout.com/trident-pegasus.

[3] https://www.dday.it/redazione/30379/exodus-indagata-esurv-spyware-play-store.

[4] https://securitywithoutborders.org/blog.html.

[5] https://www.agendadigitale.eu/sicurezza/intercettazioni-con-captatori-informatici-trojan-tutto-cio-che-bisogna-sapere/.

Articolo a cura di **Giorgio Sbaraglia**

Giorgio Sbaraglia, ingegnere, è Information & Cyber Security Advisor e svolge attività di consulenza e formazione per la sicurezza informatica, Risk Management e per il GDPR.

Tiene corsi su questi temi per molte importanti società italiane di formazione, tra le quali la Business School de Il Sole 24 Ore.

È membro del CLUSIT (Associazione Italiana per la Sicurezza Informatica) e certificato “Innovation Manager” da RINA.

Ricopre l’incarico di DPO (Data Protection Officer) per alcune aziende italiane.

È autore dei libri:

“GDPR kit di sopravvivenza” (Editore GoWare) e “Cybersecurity kit di sopravvivenza. Il web è un luogo pericoloso. Dobbiamo difenderci!” (Editore GoWare)

www.giorgiosbaraglia.it

https://www.ictsecuritymagazine.com/articoli/gli-spyware-cosa-sono-e-come-difendersi/