Authorities Takedown GozNym Cybercrime Group That Stole an Estimated $100 Million

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/L_0nDSeY8EI/authorities-takedown-goznym-cybercrime-group-stole-estimated-100-million

---

Non solo WhatsApp, anche Angry Birds e Candy Crush a rischio spionaggio

Non solo **WhatsApp**, ma anche le app di giochi che circolano in Rete sono a rischio spionaggio per gli utenti.

Dopo la criticità dell'applicazione di messaggistica fatta emergere dal *Financial Times* – dove **WhatsApp** potenzialmente permetteva ad uno ***spyware*** di prendere il controllo da remoto del nostro smartphone e ovviamente anche la sottrazione di dati sensibili – un nuovo report ha evidenziato come le app di gaming per dispositivi mobili siano a forte rischio privacy.

Come? I games invierebbero i dati personali a terze parti non ben identificate, tanto che persino gli sviluppatori delle app non saprebbero bene quali informazioni vengono inviate e a chi.

Lo spiega un report pubblicato su Vox, che ha evidenziato come molti videogame per smartphone contengono al loro interno dei

codici inseriti da altre società in quanto gli sviluppatori non costruiscono più le app da zero, ma ne prendono altre già esistenti e le personalizzano per risparmiare tempo e denaro.

Purtroppo, però, c'è un prezzo da pagare: molti videogame per smartphone nascondono dei codici che comunicano con software esterni, regalando i dati personali degli utenti. Tra le applicazioni incriminate ci sarebbero **Angry Birds** e **Candy Crush.**

Rischio privacy

Studi recenti hanno dimostrato che i giochi sono i canali preferenziali per prelevare dati personali e lanciare messaggi commerciali, anche se i dati prelevati dai giochi dovrebbero essere anonimi, nella realtà non è così. Un'inchiesta del **New York Times** ha scoperto che è molto facile de-anonimizzare le informazioni prelevate dalle app. Innanzitutto, è possibile geolocalizzare i dati, quindi risalire alla posizione della persona nello spazio. Oltre a questo, le app vengono usate sugli smartphone e quindi possono risalire a numeri di telefono, e-mail, profili social e quant'altro.

https://www.key4biz.it/non-solo-whatsapp-anche-angry-birds-e-candy-crush-a-rischio-spionaggio/258278/

Red Cross Website Hacked in

Latest Singapore Cyber Attack

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/bxq4OmCq8tA/red-cross-website-hacked-latest-singapore-cyber-attack

---

Researchers Link Disparate Chinese Hacking Groups

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/dXq91_Cocxk/researchers-link-disparate-chinese-hacking-groups

---

Report Links Vast Online Disinformation Campaign to Iran

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/fPfCNS8I4QA/report-links-vast-online-disinformation-campaign-iran

---

Leak Reveals Activity of Iranian Hacking Group

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/QEfG4083D58/leak-reveals-activity-iranian-hacking-group

---

Spyware tra interferenze illecite ed esigenze di sicurezza informatica

1. **Le intercettazioni nel codice**
2. **Le sanzioni previste dal legislatore**
3. ***Lawful Interception*: il concetto di "*prestazione obbligatoria per fini di giustizia*" e l'evoluzione delle spie telefoniche**
4. **Gli *spyware* come strumento di intercettazione**
5. **Il caso EXODUS**
6. **E' possibile difendersi dagli *spyware*?**

Le intercettazioni nel codice

In un contesto giuridico la definizione di intercettazione è offerta dalla suprema corte di Cassazione nelle linee interpretative della giurisprudenza e della dottrina in materia di intercettazioni[1], ove l'istituto va inteso come "*atto d'indagine mediante il quale, quando è indispensabile ai fini investigativi e ricorrano indizi in ordine alla sussistenza di reati a particolare allarme sociale, viene*

eseguita la captazione di comunicazioni o conversazioni riservate mediante l'ausilio di mezzi meccanici ed elettronici".

Uno strumento di ricerca della prova o di prevenzione che, nell'ordinamento interno, trova compendio negli art. 266 e 266 bis cpp laddove si tratti di intercettazioni giudiziarie, ex art. 226 att. cpp nel caso di intercettazioni preventive ed, ancora, di captazioni in materia di misure di prevenzione ex art. 78 del Decreto legislativo 06.09.2011 n. 159 e di quelle previste per agevolare le prerogative di *intelligence* riconosciute agli agenti delle due Agenzie di Informazione AISI ed AISE, ai sensi dell'art. 12 della L. 133 del 2013, che consentono la possibilità di procedere ad intercettazioni ed all'acquisizione di dati "*quando siano ritenute indispensabili per l'espletamento delle attività demandate dagli articoli 6 e 7 della legge 3 agosto 2007, n. 124".*

Le sanzioni previste dal legislatore

Fuori da questo scenario il legislatore ha disciplinato, in modo severo, ogni abuso all'uso fraudolento di intercettazioni ed alle illecite interferenze nella vita privata, sanzionando, tra l'altro:

1. chi si procura indebitamente[2], mediante l'uso di riprese visive o sonore, notizie attinenti alla vita privata;
2. chi accede abusivamente ad un sistema informatico o telematico;[3]
3. chi prende conoscenza, in modo fraudolento di comunicazioni o conversazioni (*telefoniche o telegrafiche*) comunque a lui non dirette, ovvero le interrompe o le impedisce[4];
4. chi installa apparecchiature tecniche[5], fuori dai casi previsti dalla legge, al fine di intercettare

comunicazioni e conversazioni; chi falsifica, altera o sopprime il contenuto di conversazioni[6].
5. chi detiene diffonde abusivamente codici di accesso a sistemi informatici o telematici.[7]
6. chi diffonde apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico[8];
7. chi diffonde riprese e registrazioni fraudolente[9].

Lawful Interception: il concetto di "*prestazione obbligatoria per fini di giustizia*" e l'evoluzione delle spie telefoniche

In un contesto comunitario, il 17 gennaio 1995, il Consiglio Europeo aveva adottato una risoluzione rivolta a prevenire e contrastare il terrorismo e la criminalità all'interno degli stati membri, prevedendo l'obbligatorietà, a carico dei c.d. "*gestori telefonici*", di predisposizione di un sistema di *gateways* sulle dorsali parametriche di comunicazione.

Soltanto otto anni dopo, quando il legislatore riformò il vecchio *Testo Unico delle disposizioni legislative in materia postale, di bancoposta e di telecomunicazioni* risalente al 1973, con l'introduzione del "*CODICE DELLE COMUNICAZIONI ELETTRONICHE*", nel diritto interno è stato introdotto il concetto di diritto comunitario c.d. "*prestazione obbligatoria per fini di Giustizia*" da parte dei gestori telefonici.

Sta di fatto che, da quelle due previsioni del 1995 e del 2003, è rimasta irrisolta, ad oggi, l'individuazione, *de facto*, dei gestori telefonici che non sono oggi inquadrabili in quei colossi social media che forniscono applicazioni di

messaggistica internet e di (video) comunicazione VoIP.

Una logica isterica vede *brand* internazionali come TIM, Vodafone, o Wind-H3G, -giusto per citate i marchi più noti in Italia – vincolati alla richiamata risoluzione in materia di "*prestazione obbligatoria*", a dispetto delle tante "*App*" a portata di taschino che utilizzano la connessione internet di un "gestore" al fine di consentire all'utente di "*chattare*" e videochiamare sui protocolli web (da **WhatsApp**, a **Telegram**, **Viber**, **Skype**, **Messenger** e centinaia di altri applicativi *socialmedia*), a cui vanno ad aggiungersi quelle aziende costruttrici di *device* di alta fascia, che sono in grado di sfruttare internet ed una connessione *wi-fi,* attraverso una piattaforma proprietaria di comunicazione (come ***iMessage*** e ***FaceTime*** per le piattaforme *iOS*, ed in precedenza le *chat pin to pin* ed i ***BlackBerry*** *Message (BBM)*, oggetto peraltro di diffuso interesse della giurisprudenza di legittimità)[10].

In un contesto sovranazionale e geopolitico, l'amministrazione di sistema delle *chat social media*, o dei *brand* costruttori di *devices*, è stata al centro di complesse *querelle* governative, come accaduto, ad esempio, oltre Oceano, per l'accesso, da parte del *Federal Bureau of Investigation* al contenuto di dispositivi **Apple** protetti da crittatura anti-intrusione con autodistruzione, o al fine di accedere ai server di WhatsApp, fino al recente arresto di **Meng Wanzhou**, figlia del magnate di **Huawei** accusata da Washington di "operare per minare gli interessi della sicurezza nazionale degli Stati Uniti".

Fuori dal coro l'atteggiamento collaborativo del primo vettore VoIP, **Skype**, che già nel 2011, con il passaggio a *Microsoft*, aveva messo a disposizione delle autorità governative statunitensi il brevetto "*Legal Intercept*" con*patent application* n. 20110153809, così da consentire l'installazione, in modalità nascosta, di alcuni "*agenti di registrazione*" sia sul computer del *target* oggetto di monitoraggio istituzionale, così da bypassare gli algoritmi proprietari *iLBC (Internet Low Bitrate Codec)* e *SILK (Super*

Wideband Audio Codec).

Ecco, allora, l'evoluzione dei *malicious software* – originariamente inoculati per ragioni commerciali non ortodosse – in insidiosi *spyware* di intercettazione – nel contesto giuridico denominati captatori informatici o *software* di intrusione informatica – per esigenze di captazione (sia essa legale o clandestina) di quegli sbarramenti di flussi telematici incanalati su sistemi di comunicazione sicura "lucchettati" con l'*HyperText Transfer Protocol over Secure Socket Layer* (**HTTPS**), o intellegibili solo tra gli utenti interessati con protocolli proprietari di cifratura o, ancora, protetti da tecnologie di crittografia *end to end* o *peer to peer*, (come i tanti applicativi chat social media di cui è stato fatto cenno) oggi non intercettabili dalla maggior parte dei sistemi tradizionali di intercettazione istituzionale.

La *ratio* dei "*trojan horses*" di intercettazione è quella di insinuarsi – con espedienti di *root o di jailbreak* – nel *device* acquisendone l'amministrazione di sistema per logiche di spionaggio.

In questo contesto, le tecnologie di intercettazione tattica, classificate dalla Comunità Europea come tecnologie "*dual use*" sono state disciplinate dal **Regolamento CE 1334/2000**, sulcontrollo delle esportazioni di prodotti e tecnologie *dual use*, recepito in Italia con l'adozione del **D.Lgs. 96/2003,** fino all'introduzione comunitaria del concetto giuridico di "***software di intrusione***", compendiato nel **Regolamento UE 1382/2014** ed ulteriormente disciplinato dal recente **Regolamento UE 1996/2016,** in tema di esportazione di prodotti "***dual use***", con la previsione, in caso di infrazione, di sanzioni penali di particolare fermezza.

Gli *spyware* come strumento di

intercettazione

Nelle intercettazioni a fini giudiziari gli *spyware,* o captatori informatici, ricoprono un ruolo sempre più rilevante. I metodi di intercettazione tradizionali si sono rivelati inefficaci poiché i siti *web* e i servizi di messaggistica utilizzano metodi crittografici, rendendo in questo modo le comunicazioni e i dati in transito indecifrabili; al contrario, gli *spyware* permettono di collezionare i dati alla fonte, ossia, prima di essere cifrati e trasmessi.

Per spyware o captatore informatico si intende un software, spesso sotto forma di *virus trojan*, in grado di espletare diverse funzioni utili in sede di indagini. A differenza dei *virus* e dei *worm*, gli *spyware* non sono in grado di diffondersi autonomamente, ma richiedono l'intervento dell'utente per essere installati. In questo senso sono dunque simili ai *trojan.* Il termine *spyware*, in un senso più ampio, è solitamente usato per definire un'ampia gamma di *malware*, ossia *software* maligni, dalle funzioni più diverse, quali, ad esempio, l'invio di pubblicità non richiesta (*spam*), la modifica della pagina iniziale o della lista dei Preferiti del *browser*, oppure attività illegali quali la re-direzione su falsi siti di *e-commerce (phishing).*

Molti programmi offerti "gratuitamente" su Internet celano in realtà un *malware*: il *software* è apparentemente gratuito, il prezzo da pagare è un'invasione della *privacy* dell'utente, quasi sempre inconsapevole. Spesso, la stessa applicazione che promette di liberare dagli *spyware* è essa stessa uno *spyware* o ha in realtà installato *spyware*.

Tali *malware*, quindi, si celano spesso, all'interno di altri programmi apparentemente innocui e vanno a infettare il *device target*.[11] Il captatore informatico non viene individuato dai sistemi antivirus dei *device* ove viene allocato, poiché

utilizza delle tecniche di mascheramento in grado di eludere i sistemi di rilevamento. I captatori vengono iniettati sfruttando una vulnerabilità all'interno del sistema operativo target non nota nemmeno agli sviluppatori del programma, definita comunemente "*0-day*" (in quanto il programmatore del codice vittima dell'attacco ha zero giorni per poter effettuare la correzione dopo che questo viene attaccato sfruttando una sua vulnerabilità intrinseca). Talvolta, uno *spyware* può essere installato su un *device* di un inconsapevole utente sfruttando le usuali tecniche di ingegneria sociale, che utilizzano metodi di comunicazione e di persuasione allo scopo di ottenere o compromettere informazioni personali, tramite un vero e proprio studio di ogni soggetto da intercettare.

Alcuni *spyware* vengono eseguiti solo nel momento in cui si utilizza l'applicazione di cui fanno parte e con cui sono stati installati e, dunque, la loro esecuzione cessa nel momento in cui viene chiuso il detto programma. Molti *spyware* hanno, invece, un comportamento più invasivo poiché modificano il sistema operativo del computer ospite in modo da essere eseguiti automaticamente ad ogni avvio. In certe circostanze, l'installazione di *spyware* viene eseguita in maniera ancora più subdola, attraverso pagine Web realizzate appositamente per sfruttare le vulnerabilità dei *browser* o dei loro *plug-in*. Si parla, in questo caso, di *drive by download* (o installazione tramite *exploit*).

Il captatore viene generalmente inoculato con diverse modalità:

- mediante posta elettronica: il *malware* appare come un allegato apparentemente innocuo di posta elettronica;
- mediante web: il *virus* è trasmesso tramite un download effettuato dall'utente da una pagina web;
- mediante trasferimento fisico tramite CD-ROM o un'unità USB da collegare all'apparecchio da infettare;
- mediante infezione dall'esterno attraverso connessione

dal *provider* di telecomunicazioni, falsi *update* o siti civetta, oppure tramite IMSI Catcher, anche portatili, che permettono alle forze dell'ordine di portare attacchi di tipo "*man-in-the-middle*" (MTM). Per ragioni di opportunità riguardo le procedure di attacco "istituzionali", si omettono ulteriori dettagli concernenti le tecniche di inoculazione, il cui stato dell'arte si trova in continua evoluzione per via delle "contromisure" di sovente utilizzate dai *target* per aggirare infezioni.

Una volta inoculato all'interno del sistema, il captatore può svolgere diverse attività e funzioni, tra le quali:

- intercettare chiamate vocali, *chat*, SMS, messaggi istantanei, e-mail;
- catturare immagini dallo schermo del dispositivo;
- acquisire la cronologia telefonica e la lista dei contatti;
- intercettare ciò che viene digitato sulla tastiera del *device*;
- visualizzare la cronologia delle ricerche web e "catturare" le schermate visualizzate sul dispositivo;
- registrare le telefonate effettuate anche mediante applicazioni o programmi (per es. Skype);
- effettuare *download* e *upload* di *file* sul dispositivo stesso;
- realizzare intercettazioni di tipo ambientale con attivazione del microfono;
- mettere in funzione la foto-videocamera di telefoni o computer per vedere i volti delle persone vicine;
- sfruttare i sistemi GPS per geolocalizzare i soggetti sorvegliati;
- svolgere funzioni di *key logger*;
- entrare nella rete domestica dell'utente, attraverso la password del Wi-Fi, e fare ulteriori intercettazioni.

Il caso EXODUS

È evidente la portata rivoluzionaria di questi *software* al fine di effettuare intercettazioni giudiziarie (e, purtroppo, anche di spionaggio illegale). Gli *spyware* sono la risposta allo sviluppo tecnologico, ma sono strumenti talmente invasivi e pericolosi che sollevano dubbi sulla loro affidabilità e la conciliazione con i nostri diritti umani e costituzionali. Ne è un esempio proprio il recente caso *Exodus*.

Lo *spyware Exodus*, programmato dalla società calabrese eSurv, è un *software* pensato per intercettazioni di Stato, avente come fine principale quello di raccogliere informazioni sull'utente del *device* infetto. Tale *malware* è stato diffuso per errore tramite una ventina di *app,* tutte italiane e in lingua italiana, regolarmente caricate sul *Play Store* di *Google*, i cui filtri non hanno rilevato alcuna minaccia per l'utente. In questo modo lo *spyware* avrebbe intercettato un migliaio di persone che lo hanno scaricato, in quanto contenuto in applicazioni ottenibili gratuitamente. Così, un *software* pensato per spiare legalmente criminali ha intercettato anche più di mille cittadini normali per un presunto errore di programmazione. L'inchiesta è stata condotta dalla società *no profit Security Without Borders* in collaborazione con la rivista *Motherboard.*

Exodus, la cui architettura informatica è rivolta ad intercettare contenuti criminali, è in grado di effettuare diverse operazioni sul telefono della vittima. È dotato di ampie capacità di raccolta e di intercettazione: può, ad esempio, registrare le telefonate e i suoni ambientali (attivando il microfono del telefono), scattare foto con la fotocamera, fare *screenshot*, estrarre informazioni sulle immagini della Galleria, così come copiare gli sms e i numeri di telefono in rubrica, recuperare i file scambiati con *WhatsApp,* conoscere la *password* della rete Wi-Fi a cui si è connessi, acquisire la lista di applicazioni installate e la

cronologia di navigazione, leggere la posizione attraverso il GPS, etc.
Le *cyber* intercettazioni di Stato prevedono che, dopo l'autorizzazione del giudice, l'intercettato venga indotto a scaricare lo *spyware*. Per esempio, inviando all'indagato, tramite un operatore *fake* un sms per scaricare l'*app* contenente lo *spyware*, con la promessa di uno sconto, o utilizzando altre tecniche di ingegneria sociale per indurre al *download*.

Uno *spyware* può essere nascosto anche in un aggiornamento del *firmware* del cellulare: il caso più noto risale al 2009, ed è noto con la sigla *INTERCEPTOR SS8*; allorquando il colosso delle telecomunicazioni ETISALAT (*Emirates Telecommunications Corporation*) aveva inviato un messaggio ai suoi utenti, raccomandando loro di installare un aggiornamento che avrebbe potuto migliorare le prestazioni del 3G sulla piattaforma *Black Berry*[12].

Il *software*, uno *spyware* sviluppato dalla società Californiana specializzata in sorveglianza elettronica SS8, sarebbe stato, a quanto sembra, utilizzato per monitorare gli utenti connessi su ETISALAT [13].

In generale, lo *spyware* permette, a chiunque lo controlli, di gestire a distanza il cellulare dell'utente; il controllore, però, potrebbe essere – anche se indirettamente – la società noleggiatrice che, per conto delle forze dell'ordine ha sviluppato il *software*.

Si tratta, ad onor del vero, una criticità di non poco conto se si considera che molti captatori informatici vengono oggi importati da aziende del settore che acquisiscono il *brand* dal costruttore ma non, anche, i complessivi privilegi di amministratore con le relative chiavi *software*.

Un "pasticcio" che il legislatore ha solo in parte disciplinato, in un'ottica comunitaria con un serie di

direttive sulle tecnologie *dual use* di rilevanza strategica[14]; da una focale interna con le novelle introdotte al codice di procedura penale in materia di "captazione informatica", ove sono disciplinate funzioni e caratteristiche dei *software spia****[15]***.

Tornando a *Exodus*, per un errore nel codice, questo *software* ha intercettato in modo indiscriminato qualsiasi utente che avesse precedentemente scaricato una delle *app*, presenti liberamente sullo *store* di Google, contenente il suddetto *spyware*. La causa che sembra aver scatenato tale problema è stata il mancato funzionamento del filtro per limitare l'intercettazione solo ai cellulari degli indagati (identificabili dal *trojan* tramite il codice IMEI del dispositivo).

La maggior parte delle app in questione si presentava come strumento per migliorare le prestazioni del cellulare. In seguito alla scoperta, *Security Without Borders* ha segnalato a Google la presenza dello *spyware,* che è stato rimosso in tutte le sue varianti, circa 25. Secondo Google una di queste applicazioni malevole ha raccolto oltre 350 installazioni, mentre altre varianti hanno raccolto poche decine ciascuna[16].

Tutte le infezioni sono state localizzate in Italia. Il virus gira almeno dal 2016, quindi è possibile che ci siano altre applicazioni infette che ancora devono essere scoperte. È preoccupante che alcune delle modifiche effettuate dallo *spyware* potrebbero esporre i dispositivi infetti ad ulteriori compromissioni o a manomissioni dei dati. Secondo *Security Without Borders* le responsabilità delle società sono più gravi rispetto ad un semplice errore di programmazione[17].

È sicuramente interessante capire il funzionamento del *virus Exodus*. L'infezione da *Exodus* ha inizio scaricando e installando una delle app infette. Il virus si compone di due *stage*, denominati "*Exodus 1*" ed "*Exodus 2*". Il primo ha il

compito di leggere il codice IMEI del cellulare e comunicarlo al *server* di *Command & Control****[18]***.

Security Without Borders ha scoperto che, anche se l'IMEI inviato è quello di un cellulare nuovo usa e getta, attivato solo per scopi di test, *Exodus* si attiva lo stesso, scaricando il secondo pacchetto *Exodus 2* contenente il virus vero e proprio, che inizia a "tracciare" il comportamento dell'utente. *Exodus*, volutamente o per errata programmazione, lascia diverse porte aperte e rende vulnerabile lo *smartphone* a chiunque sia connesso alla stessa rete Wi-Fi e, forse, persino alla stessa cella dell'operatore di telefonia mobile.

Supponiamo che un programma non attendibile (ad esempio *drive-by download* o qualsiasi programma *spyware*) venga scaricato da un ambiente non affidabile (ad esempio Internet) e venga installato sul sistema con conseguente violazione dell'integrità del sistema.[19] La violazione dell'integrità porta all'*escalation* dei diritti di accesso, il che si traduce in compromessi, in termini di *availability* (ad es. lo *spyware* consuma la CPU e le risorse di rete) e *confidentiality* (ad es. *cookie*, la cronologia di navigazione viene raccolta e inviata ad una parte non autorizzata). È chiaramente necessario un meccanismo che specifichi il flusso di informazioni non sicure (ad esempio programmi sospetti che accedono a file sensibili) e che applichi le politiche di sicurezza (ad esempio la rimozione del programma *spyware)* all'interno dell'*host client*.

Anche componenti benigne possono generare attività sensibili, ma la profondità e la frequenza di queste attività consentono di effettuare una distinzione dai componenti dello *spyware*. Un eseguibile benigno, ad esempio, non si nasconderebbe mai o non si ripristinerebbe da solo quando un utente tenta di disinstallarlo o rimuoverlo.

Fig.1. Un modello di invasioni di *spyware* comuni. Le frecce rappresentano un flusso di informazioni non sicuro che causa alcune violazioni di sicurezza.
Perché un *virus* creato ad arte per eseguire approfondite intercettazioni ambientali ha "colpito" anche utenti normali? Secondo l'ipotesi più diffusa, *Exodus* sarebbe stato caricato su *Play Store* affinché lo si potesse testare prima di utilizzarlo in indagini ufficiali[20].

Secondo il Garante della *privacy* Antonello Soro: "*È un fatto gravissimo. La notizia dell'avvenuta intercettazione di centinaia di cittadini del tutto estranei ad indagini giudiziarie, per un mero errore nel funzionamento di un captatore informatico utilizzato a fini investigativi, desta grande preoccupazione e sarà oggetto dei dovuti approfondimenti, anche da parte del Garante, per le proprie competenze. La vicenda presenta contorni ancora assai incerti ed è indispensabile chiarirne l'esatta dinamica*"[21].

E' possibile difendersi dagli SPYWARE?

Sicuramente, è necessario apportare dei miglioramenti alla normativa vigente al fine di obbligare queste società (come eSurv) ad adottare misure tecniche di sicurezza più stringenti, per esempio obbligando a usare cifratura con chiavi solo in possesso degli operatori giudiziari.

È importante precisare che i *malware* incidono sul funzionamento e sulle prestazioni del *device* su cui sono installati. All'attività principale degli *spyware,* ossia quella di raccogliere informazioni, si affiancano degli effetti collaterali, come la riduzione della velocità percepita dall'utente, l'occupazione di cicli di CPU e di spazio nella memoria RAM, la difficoltà di connettersi ad Internet, la presenza di tentativi di connessione non richiesti dall'utente, fino all'instabilità, a forme di *crash*

o al blocco del sistema.

Ovviamente, nessuno *spyware* ha lo scopo di rendere inutilizzabile il sistema su cui è installato, in quanto esso deve essere funzionante per poter consentire la raccolta delle informazioni. I sistemi non protetti possono accumulare centinaia di *spyware*. L'utente, il più delle volte, attribuisce tali malfunzionamenti a difetti del sistema operativo od a problemi *hardware* o a *virus*, e ricorre quindi ad azioni radicali come la formattazione e la re-installazione del sistema.

L'utilizzo di un *antivirus*, purtroppo, può non essere sufficiente a proteggere dagli *spyware*, dato che essi non sono *virus o worm*. Esistono invece specifici programmi *antispyware* realizzati proprio per rilevare e cancellare gli *spyware* dal sistema. Tuttavia, la rimozione di un componente *spyware* potrebbe comportare il malfunzionamento del *software* di cui esso faceva parte, e inoltre non tutti gli *spyware* vengono sempre riconosciuti o rimossi da *antivirus* e *antispyware*.

La strategia più efficace per difendersi dagli *spyware* è diffidare da qualsiasi *software* offerto gratuitamente da siti che non siano quelli ufficiali ed evitare di seguire i *link* contenuti nei messaggi di spam ricevuti nella casella di posta elettronica. È fondamentale anche aggiornare frequentemente il proprio sistema operativo con le *patch* rilasciate dal produttore al fine di prevenire l'installazione di *spyware* che sfruttano le vulnerabilità del sistema.

Non esiste ad oggi un modo per difendersi pienamente dagli *spyware*, ma esistono comportamenti e tecniche per limitarne almeno il raggio d'azione.

È legittimo, dunque, nutrire preoccupazioni per le accresciute potenzialità scrutatrici ed acquisitive dei virus informatici, suscettibili di ledere riservatezza, dignità e libertà delle persone, ma, dato lo stato delle comunicazioni sociali,

l’utilizzo di tecniche investigative così invasive rappresenta un adeguamento del sistema processuale alle nuove metodiche comunicative ed è ormai una necessità intrinseca per svolgere l’attività di indagine in maniera efficace, ovviamente nel caso in cui si agisca per l’accertamento di determinati reati.

Senza tali tecniche, sarebbe impossibile ottenere validi risultati dalle indagini tradizionali, stante la sempre più frequente criptazione delle comunicazioni. Solo questi strumenti permettono di penetrare canali criminali di comunicazione o di scambio di informazioni utilizzati per la commissione di gravissimi reati contro le persone. Occorre, pertanto, colmare il vuoto normativo a vantaggio dei cittadini e degli inquirenti con una compensazione che, nel salvaguardare i principi fissati, da un parte, dall’art. 8 CEDU in materia di privacy dell’individuo, trovi bilanciamento in quelle necessità di tutela e di *salus rei publicae****[22]***, fissato dall’art. 52 della nostra Carta costituzionale.

---

[1] Suprema Corte di Cassazione, Uff. del Massimario, Serv. Penale Rel. N. 55/2005 Orientamenti sulle linee interpretative della Giurisprudenza e della dottrina in materia di intercettazioni, p. 5: *“Gravi indizi di reato (art. 267 comma 1 c.p.p.). Punto di partenza della analisi è che i gravi indizi che, ai sensi dell’art. 267, comma 1, cod. proc. pen. costituiscono presupposto per il ricorso alle intercettazioni, attengono all’esistenza del reato e non alla colpevolezza di un determinato soggetto; per procedere ad intercettazione non è pertanto necessario che i detti indizi siano a carico dei soggetti le cui comunicazioni debbano essere, a fine di indagine, intercettate (Sez. VI, 18 giugno 1999, n. 9428, Patricelli F., rv 214127; sez. V, 7 febbraio 2003, n. 38413, Alvaro e altri, rv 227413). Ancor meglio precisa sez. V, 8 ottobre 2003, n. 41131, Liscai, rv 227053, che i presupposti della intercettazione sono la sua indispensabilità ai fini delle indagini e la sussistenza dei gravi indizi di reato.*

Tale secondo requisito va inteso non in senso probatorio (ossia come valutazione del fondamento dell'accusa), ma come vaglio di particolare serietà delle ipotesi delittuose configurate, che non devono risultare meramente ipotetiche, con la conseguenza che è da ritenere legittimo il decreto di intercettazione telefonica disposta nei confronti di un soggetto che non sia iscritto nel registro degli indagati. Da tale principio si è fatto discendere il corollario che "la mancata individuazione dell'autore dell'illecito in relazione al quale è disposta la intercettazione influisce sulla utilizzabilità dei suoi effetti nello stesso procedimento ai fini di prova di condotte criminose collegate". (Sez. I, 3 dicembre 2003, n. 16779, Prota ed altro, rv 227914). Si registra un contrasto in giurisprudenza sulla possibilità di utilizzare, quale indizio di reato ai fini della autorizzazione alla intercettazione, le dichiarazioni spontanee dell'indagato rese a norma dell'art. 350 c.p.p. non verbalizzate nelle forme dell'art. 357 ma annotate sommariamente in forma libera. Da un lato, sez. VI, 22 gennaio 2004, n. 14980, Picano, rv 229398, ha rilevato che queste possono essere utilizzate erga alios quali indizi nella fase delle indagini preliminari ai fini dell'autorizzazione dell'intercettazione di conversazioni o comunicazioni telefoniche nell'ambito di un procedimento per delitti di criminalità organizzata, non ricorrendo alcuna ipotesi di inutilizzabilità generale di cui all'art. 191 dello stesso codice ovvero di inutilizzabilità specifica. Dall'altro, per sez. I, 12 ottobre 1994, n. 4480, Savignano, rv. 200226, la mancata verbalizzazione, da parte della polizia giudiziaria, di atti che, ai sensi dell'art. 357, comma secondo, cod. proc. pen., dovrebbero essere verbalizzati comporta che tali atti, in quanto privi di documentazione, siano da considerare inesistenti e, come tali, indipendentemente da ogni riferimento alle categorie della nullità e della inutilizzabilità, inidonei ad essere assunti a base anche della semplice adozione di misure cautelari".

[2] Art. 615 bis c.p. *Interferenze illecite nella vita privata:* «Chiunque mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni.

Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo. I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione di investigatore privato».

[3] Art. 15 ter c.p. *Accesso abusivo ad un sistema informatico o telematico*. " Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

[4] Art. 617 c.p. *Cognizione interruzione o impedimento illeciti di comunicazioni o conversazioni telegrafiche o telefoniche:* «Chiunque fraudolentemente, prende cognizione di una comunicazione o di una conversazione, telefoniche o telegrafiche, tra altre persone o comunque a lui non dirette, ovvero le interrompe o le impedisce è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni o delle conversazioni indicate nella prima parte di questo articolo. I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale o di un incaricato di un pubblico servizio nell'esercizio o a causa delle funzioni o del servizio, ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione di investigatore privato».

Art. 617 quater c.p. *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*: «Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la

stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato».

[5] Art. 617 bis c.p. *Installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche:* «Chiunque fuori dei casi consentiti dalla legge, installa apparati, strumenti, parti di apparati o di strumenti al fine di intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche tra altre persone è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio o da chi esercita anche abusivamente la professione di investigatore privato».

Art. 617-quinquies c.p. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche: «Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro

anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater».

[6] Art. 617 ter. c.p. *Falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche*. «Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma falsamente, in tutto o in parte, il testo di una comunicazione o di una conversazione telegrafica o telefonica ovvero altera o sopprime in tutto o in parte il contenuto di una comunicazione o di una conversazione telegrafica o telefonica vera, anche solo occasionalmente intercettata, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio o da chi esercita anche abusivamente la professione di investigatore privato».

[7] Art. 615 quater. *Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici. "*Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

[8] Art. 615 quinquies. *Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o*

interrompere un sistema informatico o telematico. "Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329".

[9] Art. 617-*septies* c.p. *Diffusione di riprese e registrazioni fraudolente*. "Chiunque, al fine di recare danno all'altrui reputazione o immagine, diffonde con qualsiasi mezzo riprese audio o video, compiute fraudolentemente, di conversazioni, anche telefoniche o telematiche, svolte in sua presenza o con la sua partecipazione, è punito con la reclusione fino a quattro anni. La punibilità è esclusa se la diffusione delle riprese o delle registrazioni deriva in via diretta ed immediata dalla loro utilizzazione in un procedimento amministrativo o giudiziario o per l'esercizio del diritto di difesa o del diritto di cronaca".

[10] "*In tema di intercettazioni telefoniche, l'acquisizione della messaggistica, scambiata mediante sistema BlackBerry, non necessita di rogatoria internazionale quando le comunicazioni sono avvenute in Italia, a nulla rilevando che per 'decriptare i dati indentificativi associati ai codici PIN occorra ricorrere alla collaborazione del produttore dei sistemi operativo avente sede all'estero''* (*Ex plurimis,* Cassazione n. 52925/2016; Cassazione n. 16670/2016).

[11] Barbara Indovina, *"I captatori informatici: una riforma troppo contenuta per uno strumento investigativo così pervasivo",* Rivista di diritto dei media 2/2018.

[12] www.wired.com, Sheran A. Gunasekera, *Analizzando il SS8 Interceptor Application per il palmare BlackBerry,* ABSTRACT:

"[…] Questo documento fornisce informazioni su BlackBerry spyware conosciuto come "Interceptor." Il software è stato sviluppato dalla società Intercettazione legale SS8 ed è stato distribuito agli abbonati del gestore delle telecomunicazioni degli Emirati Arabi Uniti, Etisalat come un aggiornamento. […] Intorno l'8 luglio 2009, BlackBerry abbonati della base di telecomunicazioni UAE ricevuto Messaggio push WAP avevano richiesto loro di scaricare un aggiornamento. […].

[13] www.blog.armandoleotta.com, *BlackBerry: Update con spyware?,* 28 luglio 2008 by ArMyZ: " […] La piattaforma BlackBerry non è nuova a situazioni in cui si mette in discussione il rispetto della privacy. Questa volta la situazione è un po' diversa e riguardo un aggiornamento software. Spedito come un WAP PUSH MESSAGE, l'aggiornamento in questione istalla un file java sul dispositivo mobile. Tutto normale se questo aggiornamento, spedito agli utenti blackberry sulla rete ETISALAT negli Emirati Arabi, altro non fosse che un'applicazione in grado di intercettare sia mail che sms, spedirne una copia ad un server Etisalat, il tutto all'insaputa dell'ignaro utente che notava solo un degrado della durata della batteria. Pare che proprio questo aspetto abbia insospettito alcuni utenti e sviluppatori che ad un controllo più approfondito si sono ritrovati di fronte a questa sorpresa. L'aggiornamento era così etichettato: "Etisalat network upgrade for BlackBerry service. Please download to ensure continuous service quality." Il file JAR, firmato, faceva riferimento ad una applicazione nel percorso /com/ss8/interceptor/app […].

[14] M. Di Stefano*, Prodotti e tecnologie dual use, tra UE e giurisprudenza interna: sicurezza degli stati membri Vs esigenze di privacy*, pubblicato dalla rivista di sicurezza informatica ICT Security Magazine, articolo del 6.09.2017.

[15] M. Di Stefano, B. Fiammella, *Intercettazioni: Remotizzazione e diritto di difesa nell'attività investigativa*

(profili d'intelligence), II edizione con gli aggiornamenti del D.l.vo 216/2017", "*Collana Professionale*", ALTALEX, Montecatini Terme (2018).

[16] www.adnkronos.com, *Spyware di Stato, migliaia di italiani intercettati.* Pubblicato da adnkronos il 30. 03. 2019.

[17] A. Longo, *Più di mille italiani intercettati sul cellulare, per errore, da un hacker di Stato.*

[18] https://tecnologia.libero.it, *20 app infette da Exodus vi spiano: quali sono e come cancellarle,* Pubblicato da Libero/Tecnologia, 1. 04. 2019.

[19] Ming-Wei Wu, Student Member, IEEE, Yi-Min Wang, Member, IEEE, Sy-Yen Kuo, Fellow, IEEE, and Yennun Huang, Member, IEEE. *Self-Healing Spyware: Detection, and Remediation.*

[20] https://tecnologia.libero.it, *20 app infette da Exodus vi spiano: quali sono e come cancellarle,* Pubblicato da Libero/Tecnologia, 1. 04. 2019.

[21] A. Longo, *Più di mille italiani intercettati sul cellulare, per errore, da un hacker di Stato.*

[22] M. Di Stefano, *Salus rei publicae e terrorismo moderno: esigenze di prevenzione e contrasto* pubblicato dalla rivista giuridica ALTALEX, articolo dell'18.09.2017.

https://www.key4biz.it/spyware-tra-interferenze-illecite-ed-esigenze-di-sicurezza-informatica/257670/

Microsoft SharePoint Vulnerability Exploited in the Wild

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/tQEzQHO2uxc/microsoft-sharepoint-vulnerability-exploited-wild

---

Nigerian Cybercrime ‘Group’ Has 400 Malicious Actors

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/NEPatvdA_dQ/nigerian-cybercrime-group-has-400-malicious-actors

---

U.S. Government Details ELECTRICFISH Malware Used by North Korea

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/M5pyIvmxtHE/us-government-details-electricfish-malware-used-north-korea