# Bayer Confirms Cyber Attack But Says No Data Stolen

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/s7MKY3dTzGY/bayer-confirms-cyber-attack-says-no-data-stolen

---

# Spyware Exodus, Soro: 'L'utilizzo dei software spia va disciplinato in modo molto più rigido'

Il Garante per la protezione dei dati personali, **Antonello Soro**, ha spiegato le preoccupazioni emerse dalla vicenda dello **Spyware Exodus,** – software utilizzato da molte procure italiane per spiare legalmente i criminali – finito per 'sbaglio' nel Play Store di **Google** e che ha intercettato per errore cittadini non oggetto di indagini.

"*L'utilizzo di captatori informatici, cioè di software spia che vengono utilizzati per attività investigative da parte della magistratura sono uno strumento tecnologicamente molto avanzato e molto invasivo che da alcuni anni viene utilizzato all'interno di una disciplina non stringente* **–** ha detto Soro ai microfoni di **Radio 24.**

*"Abbiamo più volte sollecitato ai vari Governi una definizione più puntuale delle regole e delle misure di sicurezza proprio perché la potenzialità di questo software, una volta che abbia*

*infettato il dispositivo telefonico o il computer di una persona è capace di diventare un arma letale in quanto non si limita solo nelle comuni intercettazioni telefoniche, ma segue la persona coinvolta in tutte le tue relazioni".*

*"La legge"* – ha spiegato Soro – *"prevede che il magistrato dispone l'utilizzo di un captatore nei confronti di una persona sospettata di reati importanti. Questo procedimento viene affidato alla polizia giudiziaria che a sua volta utilizza soggetti o gestori con competenze tecnologiche varie. Questo è uno degli aspetti che da tempo abbiamo sottolineato come pericoloso in quanto ogni procura per tutte le intercettazioni ha la possibilità di rivolgersi a gestori del territorio più o meno affidabili. Ma proprio per questo un'arma così importante in una architettura che coinvolge troppi soggetti, la catena di responsabilità si allunga e il rischio di un incidente come quello che si è verificato cresce esponenzialmente".*

*"Noi diciamo da tempo che questa catena va accorciata"* – ha aggiunto il Garante Privacy –, *"perché l'utilizzo dei captatori deve avvenire se è possibile all'interno di competenze interne allo Stato, alla magistratura, alla polizia giudiziaria proprio per non comportare il rischio che persone del tutto estranee alle indagini vengono coinvolte in una raccolta massiva di informazioni".*

*"L'utilizzo dei captatori"* – ha concluso Antonello Soro – *"va disciplinato in modo molto più rigido. Una sollecitazione che noi abbiamo rivolto da tempo, e non si capisce perché ancora non è stato fatto nulla. Pensiamo che le intercettazioni di qualunque genere siano uno strumento potentissimo di cui la polizia e la magistratura devono disporre, ma lo devono fare all'interno di una cornice di garanzie per i cittadini con misure di sicurezza informatiche e organizzative molto severe.*

https://www.key4biz.it/spyware-exodus-soro-lutilizzo-dei-software-spia-va-disciplinato-in-modo-molto-piu-rigido/252455/

---

# Georgia Tech Breach Hits Up to 1.3 Million People

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/mWXaFDr89w8/georgia-tech-breach-hits-13-million-people

---

# Chinese Woman Carrying Malware Allegedly Got Into Mar-a-Lago

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/M4sTxZZTmZw/chinese-woman-carrying-malware-allegedly-got-mar-lago

---

# Spyware Exodus, i dati

# trovati in server all’estero. Chi ha avuto accesso?

Tanti risvolti nella storia di **Exodus**, il malware tutto italiano che ha rubato informazioni a più di 1000 utenti, in Italia.

L’inchiesta della procura di Napoli ha accertato come migliaia di messaggi, foto, video, chat e conversazioni intercettate – sia di persone indagate per conto delle procure, sia di ignari cittadini illecitamente spiati dal malware – sia finito all’estero, senza alcune protezione, in un server di **Amazon** in **Oregon**.

La Procura di Napoli ha messo sotto indagine quattro persone e ottenuto dal Gip il sequestro di due società, la **eServ** srl di Catanzaro e la **Stm srl**.

Tutto ruotava intorno al sistema spyware **Exodus**, realizzato da eSurv e commercializzato dalla Stm. Uno strumento in dotazione agli inquirenti di numerose Procure con il quale era possibile tenere sotto controllo le attività telematiche degli indagati.

## Violazione della privacy

I dati sono “disponibili a chiunque ne conosca le coordinate senza controlli o limiti”. Adesso le indagini puntano a stabilire in quanti e con quali fini abbiano avuto accesso alla piattaforma Exodus. Di certo sulla piattaforma, come precisano gli inquirenti sono disponibili *“Imei riconducibili a procedimenti penali, Imei in uso ad altri organi di polizia giudiziaria ed Imei in uso a persone da identificare”.*

Inoltre ad avere accesso erano le società che avevano stipulato accordi di commercializzazione e impiego del software Exodus, che secondo gli inquirenti sono circa una ventina.

## Quattro indagati

Le informazioni giudiziarie, però, invece di essere stoccate nelle unità di storage, venivano trasferite su un'area cloud di Amazon, illegalmente di esclusivo appannaggio della e-Surv.

I quattro indagati sono il rappresentante legale e l'amministratore di fatto di Stm srl, e l'amministratore legale e il direttore delle infrastrutture It di e-Surv. A tutti vengono contestati, tra l'altro, la violazione delle norme sul trattamento dei dati personali e la frode in pubblica attività.

## Cosa può fare Exodus

Lo spyware è in grado di effettuare numerosissime operazioni sul telefono della vittima, perché studiato appositamente per spiare, dato che il software è stato sviluppato come parte di un progetto finanziato dalla **Polizia di Stato**, destinato appunto all'impiego nelle indagini.

Il malware può registrare le telefonate, l'audio ambientale, copiare gli sms e i numeri di telefono in rubrica e leggere la posizione attraverso il gps.

## Nono solo privacy

L'accusa ovviamente è quella di violazione della privacy, ma il sospetto evidente è che siano servite anche a svolgere attività di dossieraggio e di ricatto.

Uno degli indagati ha dichiarato di aver inondato la rete col

malware spia per fare dei semplici ‘test’. Il pericolo però, che non si sa quante persone o addirittura aziende hanno avuto accesso ai dati.

https://www.key4biz.it/spyware-exodus-i-dati-trovati-in-server-allestero-chi-ha-avuto-accesso/252354/

---

# Head of Money Mule Operation Extradited to the United States

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/-UFvlw7xcyU/head-money-mule-operation-extradited-united-states

---

# Attackers Store Malware in Hidden Directories of Compromised HTTPS Sites

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/_BepkEPt7kY/attackers-store-malware-hidden-directories-compromised-https-sites

# Cybersecurity, l’Intelligence italiana cerca giovani analisti ed esperti cyber

Al via da oggi **fino al prossimo 10 maggio** il **reclutamento mirato dell’Intelligence italiana**.

Le nuove opportunità sono soprattutto rivolte per i giovani interessati a far parte del personale del Comparto Intelligence e che intendono dare un concreto contributo alla missione del **DIS**, dell’**AISE** e dell’**AISI** a tutela degli interessi strategici nazionali in campo politico, militare, economico, scientifico e industriale.

Si tratta di un’occasione che chiede ai giovani anche – spiega la nota del Ministero – una sentita adesione ai valori che caratterizzano il Sistema di informazione della sicurezza della Repubblica, tra cui la lealtà, la riservatezza, il coraggio, il segno di patriottismo, la proiezione verso il futuro.

## A chi si rivolge

La ricerca è rivolta alle eccellenze con una **formazione specifica in alcuni settori**, tra cui le discipline umanistiche, economiche, giuridiche, e internazionali. Così come rientrano anche le figure tecniche con elevate conoscenze linguistiche, che abbiano capacità di analisi, o esperienze maturate in aree, organizzazioni e/o organismi esteri.

Inoltre, a sostegno delle più recenti iniziative avviate dal governo in materia di protezione cibernetica e sicurezza informatica nazionali, la selezione include profili con qualificate competenze nei vari ambiti della **cybersecurity**, come ad esempio la ricerca, il monitoraggio, l'analisi ed il contrasto alla minaccia.

I curricula disponibili all'esito dell'attività di ricerca saranno sottoposti alle previste **procedure selettive**, articolate in un preliminare screening delle candidature arrivate, ed una seconda fase in cui vengono verificati i profili di professionalità, affidabilità e sicurezza dei candidati.

## Dove presentare domanda

Questo avviso di ricerca **non è l'unico dei canali di reclutamento** consentiti dalla legge di riforma del Comparto: per tutti gli altri profili, infatti, rimane attiva la possibilità di presentare candidature spontanee attraverso la sezione del sito **Lavora con noi**. Così come attivo resta lo scouting presso gli Atenei nazionali per neolaureati che hanno chiuso gli studi con una votazione apicale.

Per candidarsi c'è tempo fino alle 12:00 del **10 maggio 2019**

https://www.key4biz.it/cybersecurity-lintelligence-italiana-cerca-giovani-analisti-ed-esperti-cyber/252286/

---

# Exodus, tutta la storia dello

# spyware made in Italy

Per circa due anni qualcuno ha distribuito **malware** in grado di colpire i dispositivi delle vittime non solo esponendo le informazioni in essi contenute, ma anche rendendoli vulnerabili ad attacchi perpetrati da parte di terzi.

E’ la storia di **Exodus**, un malware tutto italiano che ha rubato informazioni a più di 1000 utenti, in Italia.

Sviluppato dalla società calabrese **eSurv**, che produce soluzioni per la sorveglianza, avrebbe intercettato per ‘errore’ persone non indagate.

Indagate perché questo speciale sypware è stato creato apposta per spiare persone finite sotto inchiesta, dato che il software è stato sviluppato come parte di un progetto finanziato dalla **Polizia di Stato**, destinato appunto all’impiego nelle indagini.

Scoperto dalla società **Security without borders** in collaborazione con **Motherboard,** la società si è difesa dichiarando che con **Exodus** è stato diffuso per errore sul Play Store di **Google**.

## Cosa può fare Exodus

Lo spyware è in grado di effettuare numerosissime operazioni sul telefono della vittima, perché studiato appositamente per spiare i criminali. Può registrare le telefonate, l’audio ambientale, copiare gli sms e i numeri di telefono in rubrica e leggere la posizione attraverso il gps.

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.

## Antonello Soro (Garante Privacy): 'Fatto Gravissimo'

"*È un fatto gravissimo* – ha dichiarato **il Garante della Privacy Antonello Soro** – *su cui c'è grande preoccupazione. Faremo i dovuti approfondimenti per quanto concerne le nostre competenze, poiché la vicenda presenta contorni ancora assai incerti ed è indispensabile chiarirne l'esatta dinamica*".

Una storia dai contorni in massima parte ancora oscuri che rilancia l'allarme sul "far west" delle intercettazioni di Stato.

## Il commento di Angelo Tofalo (Sottosegretario alla Difesa)

" *Se i fatti contestati risultassero aderenti alla realtà, rappresenterebbero l'ennesima pericolosa devianza nell'utilizzo di strumenti non sufficientemente monitorati da una politica poco sensibile alla gestione del dominio cibernetico*". Ha dichiarato il sottosegretario alla Difesa **Angelo Tofalo** commentando l'indagine e dicendosi "*fiducioso che la magistratura intraprenderà al meglio la propria azione accertando tutte le responsabilità, confidando sul fatto che nessuna istituzione abbia mai fatto un uso illecito del malware* ***Exodus***".*Non ci resta – aggiunge il sottosegretario – che sperare che gli investimenti in uomini e mezzi attivati in questi mesi possano contenere altre vulnerabilità di cui non abbiamo ancora evidenza*".

## Il commento di Deborah Bergamini

## (FI)

“*Sarebbe intollerabile scoprire che nello Stato qualcuno abbia potuto accedere, in maniera ingiustificata, a delle comunicazioni private violando l’articolo 15 della Costituzione. Chiederemo che venga fatta chiarezza sullo spyware Exodus e continueremo a chiedere con forza che venga istituita una Commissione parlamentare di Inchiesta sull’utilizzo dei dati degli utenti”.* Ha scritto su Facebook l’on. **Deborah Bergamini**, Vicepresidente e responsabile della Commissione Trasporti, Tlc e Poste di **Forza Italia.**

*Chi non capisce che dalla sicurezza dei dati passa il futuro della democrazia, – conclude la deputata su Fb – rischia di rimanere confinato ai margini della storia*“.

## Azienda sotto sequestro

Intanto la Procura di Napoli ha chiesto e ottenuto il sequestro preventivo della società. Si indaga per scoprire come sia stato possibile che un’applicazione, destinata ad essere utilizzata solo su richiesta e sotto il controllo della magistratura, fosse disponibile on line su “Google store”, così da ingannare ignari utenti che l’hanno scaricata sui loro cellulari e si sono ritrovati illecitamente spiati.

https://www.key4biz.it/exodus-lo-spyware-made-in-italy-finito-per-sbaglio-sul-play-store-di-google/252144/

---

# Buca di Beppo, Planet

# Hollywood Restaurants Hit by Card Breach

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Xga2a_zn6dE/buca-di-beppo-planet-hollywood-restaurants-hit-card-breach