Il Paese spiato

Dati rubati, «mercato gigantesco»

La Dda di Milano scopre un gruppo di hacker, investigatori e manager che creava dossier per «influenzare» politica e imprese
Quattro arresti e due misure interdittive: indagati Del Vecchio jr e Arpe. Violata anche la banca dati dell'Agenzia delle entrate

SIMONE **MARCER**

«Tutte le ex cariche di un certo livello entrano nel cda di qualcosa. E noi... spaziando dai carabinieri alla polizia all'esercito... abbiamo un ventaglio di ex cariche che diventano nostri clienti. In poche parole». Quelle di Nunzio Samuele Calamucci, socio di una società di investigazione privata intercettato nell'inchiesta della Dda di Milano che avrebbe scoperto un'associazione a delinquere specializzatasi nel fabbricare report con dati riservati, ottenuti violando le più importanti banche dati statali: quelle delle forze dell'ordine, dell'agenzia delle entrate, l'anagrafe nazionale, il casellario giudiziario. Parole che valgono più di un trattato sociologico: chi comanda spia. Chi ne ambisce il posto anche. L'informazione è potere, ed è un mercato dove tutti sono potenzialmente spiati: «Innumerevoli accessi abusivi», secondo quanto hanno detto il procuratore nazionale antimafia Giovanni Melillo e il capo della procura di Milano Marcello Viola, che ha coordinato le indagini del nucleo investigativo dei carabinieri di Varese. Banche, manager di grandi imprese, studi legali, esponenti delle forze delle forze dell'ordine ad alto livello erano nel portafoglio clienti della «Equalize», la creatura di Carmine Gallo, il superpoliziotto in pensione che si occupò del caso Gucci e del sequestro Sgarella, e di Enrico Pazzali, il presidente di Fiera Milano che è socio di maggioranza della stessa società fabbrica-dossier. Pazzagli che, pur non gestendo direttamente il Grande Fratello fruiva «egli per primo, dei servizi della società» per»ottenere informazioni su persone di suo interesse». Lo sottolinea il gip di Milano, Fabrizio Filice nell'ordinanza, respingendo la richiesta di misure cautelari per il presidente di Fondazione Fiera Milano. Provvedimento contro il quale la Procura farà ricorso. Quattro arrestati ai domiciliari e due misure interdittive per associazione a delinquere finalizzate alla commissione di reati informatici e di corruzione. Una sessantina gli indagati a vario titolo. Tra gli organizzatori dell'associazione e delinquere, secondo la procura ci sarebbero Gallo, l'ex poliziotto, Calamucci, l'hacker, socio di un'agenzia di investigazioni che vanta contatti con Anonymous («con loro, che sono più o meno 3 mila persone condividiamo, se c'è qualche rottura di palle... oppure vuole i dati da qualche parte...per dire... abbiamo trovato 30 account violati a chi interessano?»), Giulio Cornelli, che redigeva i dossier, un altro investigatore privato e due tecnici informatici. Poi c'erano i tre "ganci", equamente distribuiti nelle

Un momento della conferenza stampa di ieri mattina, in Procura, a Milano/*Ansa*

Per l'accusa, al vertice del sodalizio criminale, c'erano l'ex-poliziotto Carmine Gallo, che si occupò del caso Gucci e del sequestro Sgarella ed Enrico Pazzali, presidente di Fiera Milano

forze dell'ordine: un agente di polizia al commissariato di Rho, un carabiniere del Ros di Milano e un Finanziere in servizio presso la Dia di Lecce. I tre rappresentanti delle forze dell'ordine erano gli insider, che avevano accesso allo Sdi, la banca dati del Viminale che è utilizzata dalla pattuglie per i controlli sul territorio e che contiene informazioni sui provvedimenti di polizia e sulle mappe della criminalità organizzata, nonché agli archivi con le informazioni fiscali e patrimoniali. Gli altri archivi, anagrafe, previdenza, camera di commercio, li hackeravano direttamente.

Ad un centro punto però il sistema messo a punto per raccogliere e rivendere dati è stato evoluto in un software, che poteva fare a meno dell'intervento umano, ovvero del poliziotto, carabiniere, finanziere infiltrato. «Il progetto della commercializzazione della piattaforma Beyond - scrive il gip - nasce, su idea di Gallo e di Calamucci, proprio per sfruttare al massimo le potenzialità commerciali di questo sistema. Quello che essi vogliono realizzare è, infatti, una piattaforma digitale ad abbonamento (apparentemente una delle tante banche dati con motore di ricerca a cui è possibile abbonarsi pagando un canone), mediante la quale il cliente possa effettuare direttamente la ricerca nominativa della persona sulla quale vuole un report reputazionale». Si tratta di un aggregatore di dati riservati, ed è la svolta. La fabbrica dei dossier diventa anche la fabbrica dei soldi: «...tutta Italia inc...amo, esci fuori con un bando a venticinque euro e se compri mille crediti te lo facciamo a venti.., e tu vai avanti. Otto mesi, facendo un botto di grano...al nono mese gli hai recuperati!... Tu vedi che questo posto viaggia giorno e notte», dice Calamucci a Gallo. Il denaro non dorme mai per loro era realtà. E se devi rischiare di andare in galera, tanto vale farlo per un buon affare: «Ti fai la galera? Dopo un milione e un euro, allora inizio a parlare di qualcosa che può non essere completamente legale. Noi facciamo un conteggio... con due milioni per uno, non riusciamo a sparire?...Perché poi devi sparire! Dici sì, va boh, lo faccio... consapevole che lo stai facendo, ma mica per trecentomila euro». Questi invece è Cornelli, l'uomo dei report, ad essere intercettato. Report che venivano fatti figurare come notizie raccolte da fonti aperte, da articoli di giornale. In altri casi ai clienti che chiedevano, se fosse legale il materiale raccolto, veniva detto che la società aveva degli accrediti con i ministeri che permettevano l'accesso ai dati riservati. E gli utenti si sentivano perlopiù liberi di crederci.

Centinaia di migliaia gli spiati. Tra i "clienti" del "sodalizio" che procedeva a infiltrarsi, anche i manager di società come Erg, Heineken e il responsabile della sicurezza della Barilla

Nel portafoglio clienti che si sarebbero avvalsi dei servizi della società c'erano, tra gli altri il banchiere Matteo Arpe e Leonardo Del Vecchio Junior di Luxottica (indagati), manager di Erg e della Heineken, un responsabile sicurezza della Barilla. Tra i servizi offerti dalla Equalize c'era anche il monitoraggio del traffico dati dei dipendenti delle società, il phishing attraverso falsi profili Facebook, il controllo e la diffusione di notizie create ad arte per condizionare asset societari. Gli spiati sarebbero centinaia di migliaia. Tra i nomi illustri random: Letizia Moratti, Alex Britti, il presidente del Milan Paolo Scaroni, l'ex presidente di fiera Milano Giovanni Gorno Tempini.

Ad un certo punto il giochino era diventato così potente che i suoi gestori hanno dovuto mettereil parental control al loro socio di maggioranza, lo stesso Pazzali, che chiedeva solo per sé migliaia di report: «Non lo deve sapere», che ora si può entrare nello Sdi della polizia come se fosse Google Chrome «e non lo saprà mai... perché se sa lo Sdi siamo f...i».

L'analisi

DANILO **PAOLINI**

LA CAPACITÀ D'INDIGNARSI VALE PIÙ DELLE PASSWORD

La maiuscola, le minuscole, caratteri speciali come se piovesse (che poi vatteli a ricordare), qualche cifra che non sia quella dell'anniversario o del compleanno. Che cosa non si fa per proteggere i propri accessi al mondo digitale, che un tempo era detto virtuale e ora è tutt'uno con quello reale. Ma è roba da ridere - meglio, da piangere - a quanto pare. Di molto reale, pure troppo, c'è invece la facilità con la quale questi accessi, e i dati che dovrebbero proteggere, possono essere violati, diffusi, comprati, venduti, utilizzati per fini di cui è davvero arduo immaginare la liceità. Con tanti saluti alla riservatezza e alla sicurezza delle comunicazioni, delle transazioni economiche, dei bilanci aziendali e perfino delle relazioni amorose. In pochi mesi abbiamo avuto in Italia lo scandalo degli accessi seriali non autorizzati alla Direzione nazionale antimafia, il caso del bancario pugliese che spiava i conti di vip e conoscenti, il giovanissimo hacker siciliano che è riuscito a entrare nel data-base del ministero della Giustizia e ha messo le mani sulle password di 46 procuratori e sostituti procuratori. E l'inchiesta di Milano, che sta esplodendo in queste ore. È l'ennesima dimostrazione di quanto siano a rischio le banche dati alle quali ormai affidiamo le nostre esistenze. E di quanto potere abbiano coloro che sono in grado di ottenere quei dati, o perché sono funzionari infedeli (di una banca, dello Stato, talvolta "ex" con zero scrupoli e tanti zeri sul conto corrente) o perché sono autentici pirati dei mari telematici. Del resto, il mercato delle informazioni riservate «è gigantesco», come ha ricordato ieri il procuratore nazionale Antimafia Giovanni Melillo. Una fiera dei dossier, con clienti sempre pronti a sganciare somme cospicue per procurarsi ciò che può favorirli nell'aggiudicazione di appalti o rovinare un concorrente fastidioso. È il mercato nero contro le vere regole del mercato, che infatti spesso restano, purtroppo, lettera morta. Una tentazione enorme per chi ha l'occasione o le capacità di impossessarsi dei lingotti digitali di questa immensa miniera d'oro. Giustissimo e sempre più necessario, ovviamente, investire di più in cybersicurezza, come intende fare il governo. Ma se chi vuole aprire la cassaforte ha già in tasca la combinazione, l'impressione è che ci sarà comunque poco da fare. Ovvero, ci sarebbe tanto da fare, ma in termini di etica pubblica, di coscienza civile e di onestà, che è personale proprio come la responsabilità penale. Forse, tuttavia, prima bisognerebbe recuperare la capacità, individuale e collettiva, di indignarsi.

Per ora (e per una volta, verrebbe da dire) pare che la politica ne resti fuori, ma il mondo dell'economia e della finanza è investito in pieno dal ciclone. Sulla fondatezza delle accuse rivolte ai numerosi indagati, ovviamente, si esprimerà la magistratura. Però suscita davvero tristezza pensare che in un Paese dove tanti stipendi sono sotto la soglia di dignità, dove la precarietà del lavoro e la sua insicurezza sono autentiche piaghe sociali, dove si chiudono fabbriche alla velocità di un clic, dove si delocalizza e si cedono rami d'azienda mandando a casa migliaia di lavoratori, manager e imprenditori avrebbero speso «centinaia di migliaia di euro» - parole del procuratore di Milano Marcello Viola - per comprare informazioni ottenute illegalmente. Uno dei procacciatori e venditori di tali informazioni, intercettato dagli inquirenti, avrebbe detto che l'intento era quello di «fregare tutta l'Italia» e di «tenere in mano il Paese». Speriamo che il Paese riesca a divincolarsi.

L'INDAGINE

È uno scenario molto più che inquietante quello che viene fuori dalle carte dell'inchiesta, che coinvolge una sessantina di persone. Ecco come «la fabbrica di report diventava fabbrica di soldi»

L'ALLARME

Italia vulnerabile: i nostri archivi elettronici sono tra i più violati

Preoccupa l'ultimo report dell'Osservatorio Cyber del Crif. «Mai condividere i propri dati online», consiglia la direttrice Rubini

ILARIA **SOLAINI**
Milano

L'Italia è al quinto posto per furto di email e password online ed è al settimo posto per numero di indirizzi email compromessi. E per quanto riguarda i dati frodati delle carte di credito in circolazione, l'Italia si colloca al 18° posto nella classifica mondiale. Nei primi sei mesi 2024, inoltre, è aumentato del 10% il numero di *alert* relativi al rischio che i propri dati finiscano in mano a criminali informatici e, in particolare, nel dark web, quella zona grigia in cui le potenzialità del web sono sfruttate a scopi illegali. In sintesi, questi recenti dati che arrivano dall'Osservatorio Cyber del Crif, che analizza la vulnerabilità degli utenti e delle aziende agli attacchi informatici, ci dicono fondamentalmente che siamo tutti esposti ai rischi correlati alla circolazione online dei nostri dati personali. Nel 2023 gli investimenti nella cybersecurity sono cresciuti del 12,4% arrivando a 1,8 miliardi di euro, eppure la Corte dei conti europea, settimane fa, aveva messo nero su bianco le sue perplessità sull'operato dell'Italia nella sicurezza informatica: per una gestione efficace dei rischi informatici non è sufficiente analizzarne l'impatto era stato il verdetto in sintesi e l'invito al nostro Paese a lavorare su «azioni concrete per l'implementazione di politiche e procedure di sicurezza, per la gestione degli incidenti, per le procedure di test, per l'efficacia delle misure adottate, la formazione del personale». In sintesi, bisogna crescere in protocolli di prevenzione, ma soprattutto in formazione all'università e non solo.

Anche a livello personale, si può fare qualcosa per migliorare la protezione dei propri dati online: «Bisogna prestare particolare attenzione alle email e ai messaggi che riceviamo ogni giorno, allenandosi a riconoscere i tentativi di truffe e *phishing*. È importante non cliccare sui link contenuti nelle email o negli SMS sospetti e, soprattutto, non rispondere fornendo dati personali a messaggi apparentemente inviati dalla nostra banca o da un'altra azienda, controllando sempre il numero di telefono o l'indirizzo email del mittente», ha spiegato Beatrice Rubini, Executive Director di Crif.

Tra le informazioni ritenute sensibili ci sono, ad esempio, la data di nascita, il codice fiscale, l'indirizzo di residenza, gli account di social media e il numero di telefono, diventato un dato personale sempre più prezioso e da tutelare maggiormente. Che cosa può accadere in caso di un accesso non autorizzato alla nostra posta elettronica? Tra i dati, ad esempio, potrebbero esserci anche le credenziali dei nostri account personali o aziendali, che usiamo per accedere a servizi online come l'*home banking*. Poi c'è il rischio spam, vale a dire che le nostre informazioni rischiano di essere usate per l'invio di email ingannevoli tese a ottenere ulteriori informazioni personali o credenziali di accesso. Che fare, dunque, per far sì che i nostri account non vengano violati? Ad esempio, le impronte digitali o le scansioni facciali sul computer o sullo smartphone sono più sicure rispetto ai codici di accesso che possono essere facilmente indovinati e offrono agli aggressori maggiori opportunità di compromettere i nostri dispositivi. È importante, inoltre, utilizzare l'autenticazione a più fattori (MFA) ogni volta che è possibile, poiché fornisce un elevato livello di sicurezza che rende più difficile l'accesso ai propri account da parte di *hacker* e criminali informatici. E infine, bisogna prestare attenzione a non incorrere in errori banali come condividere pubblicamente informazioni personali, anche in modo ingenuo, magari in post pubblici sui social media, oppure in sondaggi su Facebook. «Bisogna mantenere alta l'attenzione ogni qualvolta veniamo invitati a fornire dati personali e adottare strumenti di protezione», è il consiglio finale di Rubini.