Rassegna stampa

Centro Studi C.N.I. - 11 luglio 2015

Waypress
media monitoring

EDILIZIA

INGEGNERI IUNIOR

SEMPLIFICAZIONI

SICUREZZA ICT

MICROCREDITO

MAFIA CAPITALE

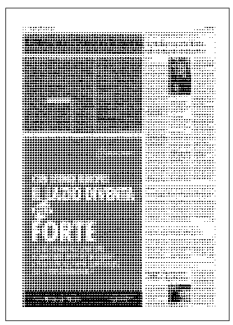
SICUREZZA ICT

Ance: subito lo sblocca-opere per la ripresa

L'edilizia non riparte: investimenti ancora giù

L'edilizia ancora non riesce a uscire dal tunnel: l'associazione nazionale dei costruttori (Ance) prevede nel suo Osservatorio congiunturale un'ulteriore caduta degli investimenti in costruzioni dell'1,3% per il 2015, mentre il 2016 parte da un -0,5% e potrà andare in positivo solo in presenza di politiche di rilancio. A questo proposito, Ance considera urgente ma anche realistico lo sblocca-opere da 20 miliardi: 15 miliardi ci sono già e vanno attivati, altri 4,5 vanno trovati.

Giorgio Santilli ▸ pagina 16



Osservatorio congiunturale. Per i costruttori non mancano segni positivi: ad aprile ore lavorate +0,6%

Edilizia, non c'è ancora la ripresa

Ance: nel 2015 -1,3%, 2016 a -0,5% - «Subito lo sblocca-opere di Renzi»

Giorgio Santilli
ROMA

L'edilizia non è ancora uscita dal tunnel della crisi più lunga del dopoguerra, nonostante non manchi qualche segnale di risveglio, come l'aumento delle ore lavorate (+0,6%) ad aprile. Per l'Ance, l'associazione nazionale dei costruttori che lunedì presenterà l'Osservatorio congiunturale semestrale, il 2015 segnerà un altro dato negativo dell'1,3%. Per il momento, e in attesa di capire cosa ci sia di reale negli annunci di Matteo Renzi di voler «sbloccare opere per 20 miliardi», l'Ance conferma una previsione negativa anche per il 2016: -0,5 per cento. I costruttori prevedono, tuttavia, che la ripresa potrà effettivamente arrivare nel corso del prossimo anno - dopo nove anni di segno negativo - se il governo farà la sua parte con una politica di maggiore attenzione agli investimenti pubblici e all'incentivazione degli investimenti privati.

Per accelerare verso il bel tempo basterebbe che si trasformassero in realtà gli annunci fatti nei giorni scorsi dal Presidente del Consiglio e dal ministro delle Infratsrutture, Graziano Delrio. E su questo punto l'Ance presenterà lunedì un lavoro che "aiuta" (e al tempo stesso incalza) il governo a trovare misure, fonti di finanziamento e progetti che possono confluire nel piano sblocca-opera.

Dalla puntuale tavola dell'Ance, che evidenzia investimenti possibili (nuovi o da sbloccare) per un totale di 19,4 miliardi, si evince che stavolta lo sblocca-opere renziano è credibile e realistico, a condizione che si prendano alcune misure necessarie. In sostanza, dice l'Ance, 14,9 miliardi di lavori si potrebbero sbloccare soltanto dando attuazione a provvedimenti già approvati o in corso, mentre 4,5 miliardi di investimenti potrebbero arrivare da progetti e proposte già all'attenzione del Ministero delle Infrastrutture, per cui però, è necessario trovare il finanziamento. In sostanza - dice ancora l'Ance - lo sforzo del governo in termini finanziari dovrebbe essere di 4,5 miliardi mentre per il resto le risorse ci sarebbero già o sarebbero già programmate da vecchi provvedimenti. Vediamo il dettaglio di questi programmi finanziati e da sbloccare.

La posta più cospicua è il contratto di programma di Rfi che vale 4 miliardi di investimenti attivabili, già finanziati con legge di stabilità 2015, decreto legge sblocca-Italia di fine agosto 2014 e fondi europei.

A conferma che c'è un grosso problema di attuazione del decreto legge sblocca-Italia, a più di dieci mesi di distanza dall'approvazione, altri tre miliardi da avviare riguarderebbero i cantieri medio-grandi previsti da quel provvedimento e altri 500 milioni per le opere medio-piccole. Anche la terza voce, per dimensione, dello studio Ance riguarda un piano che il governo considera assolutamente prioritario da molti mesi: si tratta del piano contro il dissesto idrogeologico che potrebbe portare a opere per tre miliardi ma che stenta a decollare noonostante lo sforzo straordinario dell'unità di missione di Palazzo Chigi. Qui si tratta di vecchie risorse (2,4 miliardi) non utilizzate per ritardi regionali e di 600 milioni già deliberati dal Cipe per il piano stralcio delle città metropolitane (si veda il Quotidiano Edilizia e Territorio per l'elenco dei 35 interventi contenuti nel piano stralcio).

Ci sono poi altri due piani di media dimensione che da tempo sono pronti al decollo ma che non partono: il piano dell'edilizia scolastica (per una prima tranche di 1,2 miliardi) e il contratto di programma Anas (1,1 miliardi) che da quest'anno punta molto più che in passato sulle opere di manutenzione. Quanto al piano dei porti (0,9 miliardi), è stato appena approvato dal Consiglio dei minstri e punta su fondi europei 2014-2020. Infine, il piano dell'edilizia abitativa (500 milioni), gli investimenti per il trasporto pubblico locale (300 milioni) e il piano aeroporto (200 milioni da trovare).

IL QUADRO DELLE RISORSE
Per sbloccare i 20 miliardi di lavori di cui ha parlato il premier bisogna trovare nuovi fondi e solo per 4,5: gli altri ci sono e devono essere attivati

Piano Renzi

Programmi da sbloccare secondo le indicazioni del governo

	Importo in mld €
Contratto di Programma Rfi	4,0
Sblocca Italia - 4 programmi di opere medio-piccole	0,5
Sblocca Italia - Altri cantieri (medio-grandi)	3,2
Dissesto idrogeologico	3,0
Edilizia scolastica	1,2
Contratti di Programma Anas	1,1
Piano dei Porti	0,9
Piano edilizia abitativa	0,5
Trasporto Pubblico Locale	0,3
Piani degli aeroporti	0,2
Cantieri dei Provveditorati ed eventuali cantieri selezionati dal Mit nell'ambito del Piano Ance	4,5
Totale	**19,4**

Nota: gli importi indicati sono quelli dichiarati dal Governo nella prima parte del mese di luglio. Le principali fonti di finanziamento sono indicate da Ance
Fonte: elaborazione Ance

Il Tar Campania estende le prerogative degli iscritti alla sezione B

Ingegneri junior tutelati

Possono firmare offerte tecniche migliorative

DI DARIO FERRARA

Anche l'ingegnere junior può firmare l'offerta senza far perdere la gara alla sua impresa se si tratta di migliorare un progetto già indicato in via generale dalla stazione appaltante. È quanto emerge dalla sentenza 797/15, pubblicata dalla seconda sezione del tribunale amministrativo regionale della Campania, sezione di Salerno.

Collaborazione consentita

Niente da fare per l'azienda arrivata seconda nella procedura bandita dal Comune per la realizzazione di lavori per le fogne e l'impianto di depurazione: fallisce il tentativo di far revocare l'aggiudicazione alla concorrente sul rilievo che l'ingegnere junior non avrebbe avuto i titoli per firmare l'offerta tecnica. Nel caso di specie l'offerta economicamente più vantaggiosa per l'amministrazione è individuata in base alla presentazione di progetti capaci di individuare soluzioni tecniche migliorative della rete fognaria e dell'impianto di depurazione.

Il documento contestato, dunque, s'innesta su un progetto già redatto dalla stazione appaltante e che nella sua intima struttura non può essere modificato ma soltanto migliorato.

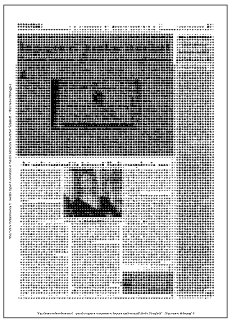
I paletti posti dalla normativa all'ingegnere junior nascono per evitare che al professionista con una qualifica «ridotta» possa essere affidata la progettazione di opere pubbliche complesse.

Ma per il settore ingegneria civile e ambientale chi è iscritto alla sezione B del dpr 328/01 ben può porre in essere attività di concorso e collaborazione alle attività di progettazione, direzione dei lavori, stima e collaudo di opere edilizie.

In base alla legge l'ingegnere junior può occuparsi anche di: progettazione, direzione dei lavori, vigilanza, contabilità e liquidazione relative a costruzioni civili semplici con l'uso di metodologie standardizzate.

Ed è anche titolato a compiere i rilievi diretti e strumentali sull'edilizia attuale e storica e i rilievi geometrici di qualunque natura. È esattamente ciò che avviene nel caso delle fogne e del depuratore da ristrutturare su indicazione del Comune campano nell'ambito del progetto già esistente, che non può ritenersi un'attività di competenza esclusiva degli ingegneri appartenenti alla sezione A.

All'azienda esclusa non resta che pagare le spese di giudizio.



Un tavolo di confronto tra le istituzioni e le categorie professionali

Verso vere semplificazioni

Ridurre del 30% i costi a carico delle imprese

DI LUCIA BASILE

Semplificazioni, al via il tavolo ministeriale con le categorie professionali. Convocati, tra gli altri, i rappresentanti di Rete Imprese Italia a cui aderisce la Lapet nell'ambito di Cna Professioni. L'obiettivo è quello di raccogliere proposte e suggerimenti per arrivare a ridurre del 30% i 17 miliardi di costi da adempimento oggi sostenuti da piccole e grandi imprese. Ulteriore obiettivo è quello di arrivare alla definizione di una calendario degli obblighi tributari in cui si evitino scadenze ravvicinate e le continue richieste di proroghe. Un tavolo al quale i tributaristi avranno modo di portare le loro istanze, attraverso Rete Imprese Italia, raccolte nell'ambito delle dieci proposte avanzate da Cna Professioni a governo e Parlamento per migliorare la vita dei professionisti. Al punto 1 del decalogo primeggiano infatti le semplificazioni fiscali. La revisione degli adempimenti, in particolare di quelli superflui, è uno dei temi caldi sul quale la Lapet si è più volte espressa. «Troppi adempimenti, scadenze incerte, leggi contraddittorie, e solo per citare un caso di estrema attualità, il modello 730 precompilato, senza considerare il fatto che il forte aumento della pressione fiscale, registrato in questi anni, ha creato non poche difficoltà ai cittadini, ai professionisti e alla stessa Pubblica amministrazione», ha ricordato il presidente nazionale Lapet Roberto Falcone. «Abbiamo da sempre sostenuto la necessita di assumere decisioni, coraggiose e tempestive che possano influire positivamente sul pil, quali la riduzione dei costi della burocrazia e della spesa pubblica improduttiva dello stato» ha aggiunto il presidente, «la burocrazia infatti, continua ad essere una vera e propria tassa occulta, un ostacolo oltreché un onere per cittadini e imprese. Perché un imprenditore dovrebbe investire in Italia, uno dei Paesi con la tassazione più alta e la burocrazia più gravosa d'Europa?». Un altro impegno riguarda la questione dell'attuazione della delega fiscale. Sotto i riflettori la formulazione dell'attuale schema di dlgs sul contenzioso. A tal riguardo, potenziamento degli strumenti alternativi di risoluzione delle controversie ed estensione delle categorie ammesse al patrocinio tributario, sono le indicazione dei tributaristi. «La condivisione delle nostre proposte da parte delle forze politiche, rappresenterà un atto di giustizia nei confronti di professionisti qualificati, quali i tributaristi Lapet, oggi riconosciuti grazie anche alla legge 4/2013», ha auspicato Falcone.

L'Associazione quindi auspica che l'insediamento di questo tavolo possa rappresentare l'apertura di un fronte comune da parte di tutte le categorie economico-contabili, al fine di programmare e condividere un piano che tra i punti comuni preveda, in primis: lotta all'eccesso di burocrazia e incentivo alle reali semplificazioni. I tributaristi dunque si dicono pronti a continuare a promuovere tutti quei provvedimenti che vanno nella direzione poc'anzi descritta: «siamo disponibili a mettere a disposizione la nostra competenza in qualità di esperti del settore ai tavoli tecnici in materia, come quello appena insediato, affinché il legislatore possa attuare misure rivolte al rilancio economico e sociale del nostro paese».

la Repubblica

I segreti bruciati di Hacking Team "Palazzo Chigi fece pressioni per noi"

MARCO MENSURATI
FABIO TONACCI

ROMA. L'unico indizio che ha in mano la procura di Milano per risolvere il caso è un indovinello. Scritto in inglese sul profilo Twitter di Phineas Fisher, l' "ombra" che il 6 luglio, per primo, ha rivelato al mondo l'attacco informatico alla società milanese. Tradotto, suona così: «Scriverò come l'Hacking Team è stato bucato solo quando avranno fallito il tentativo di capire cosa è successo e saranno fuori dal mercato».

Sono passati cinque giorni da quel tweet, e ancora nessuno sa come sia stato possibile rubare 420 gigabyte di dati riservati, compreso il codice sorgente del software spia Galileo anche noto come Rcs, usato dalle polizie e dai servizi segreti di molti Stati, tra cui l'Italia. Un furto diventato materia di sicurezza nazionale da quando,ieri, quattro anni di corrispondenza interna dei dipendenti di Ht srl (circa un milione di email in tutto) sono stati rilanciati da Wikileaks. Si tratta solo di una piccola parte di quei 420 giga, che sono comunque facilmente scaricabili da Torrent e che in queste ore stanno disintegrando indagini, segreti nazionali, identità di agenti segreti. Un calderone che sta svelando, tra l'altro, contatti proibiti della società con decine di governi dittatoriali quali Etiopia e Sudan. Materiale imbarazzante, come i documenti che dimostrano la "benevolenza" di Palazzo Chigi nei confronti dell'azienda milanese.

IL MISTERO DI PHINEAS

Il procuratore aggiunto di Milano Maurizio Romanelli, che sta indagando sul caso insieme alla Polizia Postale, non si sbilancia. Ma la storia di Phineas Fischer e del gruppo di "hacktivisti" in guerra con i fiancheggiatori dei Paesi a democrazia zero non convince del tutto. Indovinello a parte, non c'è stata una rivendicazione chiara sul Web, né proclami ideologici. Pure la dinamica dell'attacco genera qualche dubbio. Tutto troppo facile. Succhiare 420 gigabyte richiede tempo, possibile che nessuno se ne sia accorto? A quanto se ne sa, le password per accedere al sistema ("hackerteam2015" e "passw0rd") sarebbero state trovate hackerando il profilo twitter di un dipendente amministratore di sistema, e una volta dentro i dati non erano protetti da alcuna forma di crittografia. L'impressione è che sia più probabile che tutta questa storia non sia altro che un capitolo, il primo che colpisce il nostro Paese, di quella cyberguerra in corso ormai da anni, il cui scenario è ancora in via di definizione.

LA PROLIFERAZIONE DI GALILEO

Il software dell'Hacking Team è un prodotto semplice e micidiale. Infetta il computer (o telefono o tablet) su cui viene scaricato e succhia tutte le informazioni che passano di lì, dirottandone una copia sul computer dell'intercettatore. In teoria può essere anche utilizzato al contrario, e cioè per installare sul dispositivo infetto file (foto o testi) all'insaputa del proprietario. Non solo: chi lo studia da anni è sicuro che abbia anche una backdoor, una "porta sul retro" dalla quale, oltre al cliente, non solo il fornitore del software (cioè l'Hacking Team) ma anche qualche servizio segreto interessato al controspionaggio può in teoria leggere le informazioni.

Il problema nasce quando un'arma tanto potente entra in possesso di troppa gente. Che è quello successo con Galileo. «Nel 2007 - racconta una fonte investigativa di Repubblica - mi occupavo di traffico internazionale di droga ed eravamo tutti nel panico perché i trafficanti per non essere intercettati comunicavano via Skype. Quelli di Ht erano gli unici ad aver sviluppato un prodotto ad hoc. Stavano per venderlo con vincolo di Segreto di Stato ai servizi segreti italiani. Nel 2012 scaduto il vincolo del Segreto di Stato, per una questione di business, avevano scelto di darlo a terzi i quali a loro volta lo cedettero ad altre due compagnie».

"Per motivi di business", l' "arma" aveva cominciato a girare.

LE FATTURE E LE MAIL

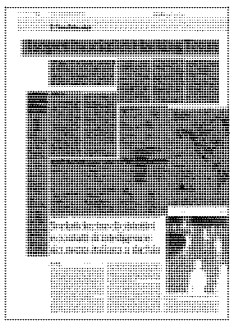
Non solo in Italia, ma in tutto il mondo. E per i soliti motivi di business anche nei Paesi a "democrazia zero" o quasi: Libano, Sudan, Arabia Saudita, Kazakistan, Oman, Mongolia, Russia, Tunisia, Turchia, Nigeria, Bahrain ed Emirati Arabi. Le mail divulgate da Wikileaks e i file di Torrent sin qui noti sono abbastanza eloquenti. C'è la fattura della seconda tranche del pagamento da parte dei servizi del Sudan (collaborazione sempre negato dall'Hacking Team). E la pistola fumante del "caso etiope". Nel marzo di quest'anno, un gruppo di giornalisti etiopi ha denunciato di aver subito un attacco informatico da parte del governo, attraverso i sistemi dell'Hacking Team. Il governo smentì, Ht non disse nulla.

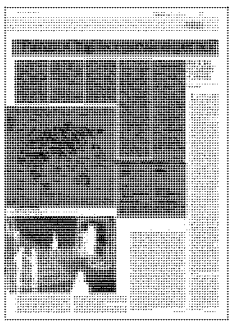
Oggi saltano fuori mail imbarazzanti: «Hanno trovato la sorgente dell'attacco - si scrivono tra di loro i tecnici della Ht in quei giorni - perché questi furboni hanno usato lo stesso indirizzo email che avevano già usato in un precedente attacco per inviare il doc con l'exploit (cioè il file infetto). Direi che questa e' l'ultima che ci combinano (...) Tra l'altro hanno identificato il vecchio collector perché queste scimmie hanno deliberatamente il firewall aperto».

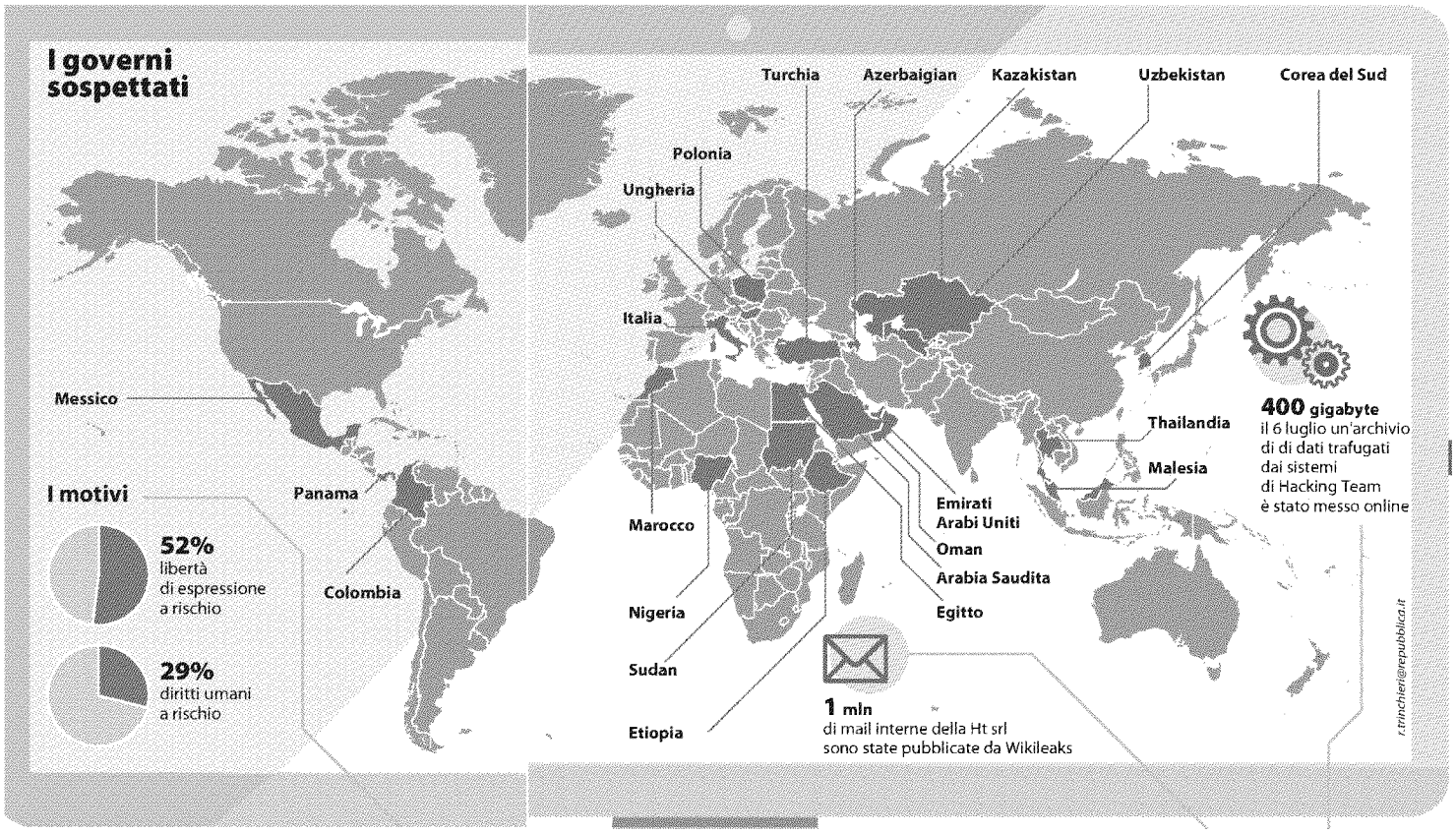
LA PRESIDENZA DEL CONSIGLIO

Reporters sans frontières e altre associazioni avevano più volte puntato l'indice contro Ht. Ciò non ha però impedito al governo italiano di tutelare gli interessi di David Vincenzetti & co., anche in sede istituzionale. E di esserne cliente, come dimostra una fattura di 33.625 euro del maggio 2014 intestata alla Presidenza del Consiglio.

Un'attenzione spiegabile anche con una forma di real politik: non capita spesso a una intelligence come la nostra che una società italiana si ritrovi al centro, almeno potenzialmente, di un turbinio di informazioni del genere. E che disponga di un software moderno, richiesto e utilizzato dai servizi di mezzo mondo. Un idillio che rischia di interrompersi il 30 ottobre scorso, quando il governo si accorge che Galileo è un prodotto del tutto simile alle armi. E pertanto, la sua commercializzazione all'estero deve essere autorizzata dal Ministero per lo sviluppo economico, che deve valutare se i Paesi destinatari siano inclusi nelle liste di embargo. La procedura si blocca. E con essa gli affari dell'Hacking Team, che rischia il collasso. L'amministratore delegato Vincenzetti attiva tutti i suoi contatti: «Ieri - scrive - ho parlato con diversi miei contatti Governativi (...) Alcuni di essi ora non lavorano più presso i nostri attuali clienti ma si sono spostati più in alto e sono vicini ai vertici assoluti del Governo — ovviamente si occupano di sicurezza nazionale». E ancora: «Stiamo facendo la massima pressione possibile. Nell'ambito di questa attività ho interloquito tra ieri e oggi, e si stanno interessando alla cosa, Aisi, Ros, Polizia e Aise». Infine la vittoria: «Non sappiamo con esattezza da dove sono arrivate le pressioni maggiori al Mise. Ma su una posso giurarci: la Presidenza del Consiglio».







Viaggio tra misteri e pericoli del software spia. Milioni di email pubblicate. E il giallo su chi ha sferrato l'attacco

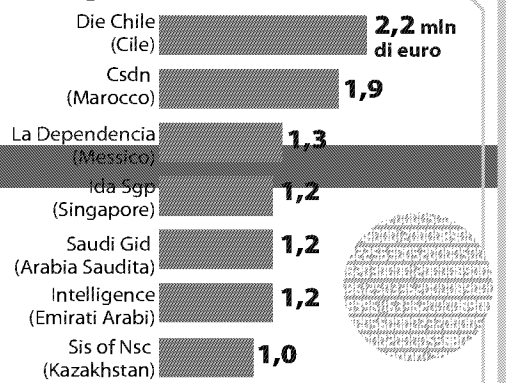
Hacking Team

2003
anno di fondazione della società che produce software spia

74
cilenti nel mondo (2015): agenzie di spionaggio, governi, polizie

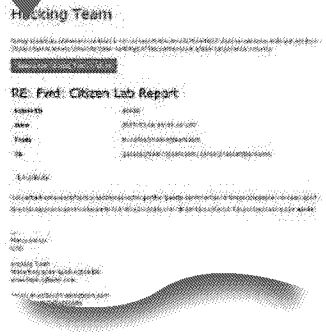
41 mln di euro
il fatturato previsto per il 2015

I "migliori" clienti

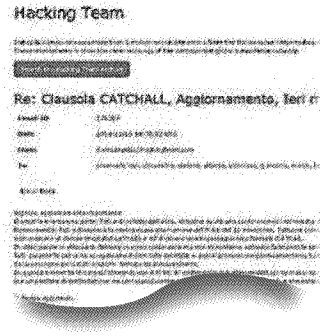


FONTE DATI CONTENUTI NEI FILE RUBATI AD HACKING TEAM E DIFFUSI IN RETE

I CASI



I SERVIZI SEGRETI ETIOPI
"Queste scimmie hanno il firewall aperto": Hacking team si lamenta così del modo in cui i servizi etiopi usano il software



LE PRESSIONI SUL MINISTERO
"Stiamo facendo la massima pressione possibile". Al ministero dello sviluppo economico, per l'esportazione del software spia

Il software
Remote Control System (Rcs- Galileo) permette di controllare pc o smartphone da remoto

In Italia
il software spia è utilizzato da Carabinieri, Polizia Postale e Guardia di Finanza

LE TAPPE

1

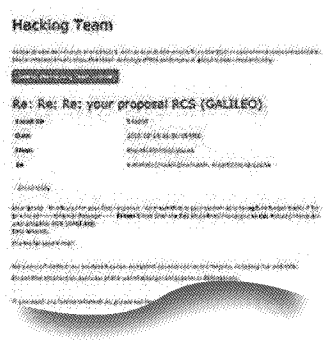
L'INFEZIONE
Hacking Team, con sede a Milano, vende software-spia tra i più sofisticati in circolazione che "infettano" sia Windows, sia Mac e smartphone, a governi e polizie in Italia e all'estero

2

LE ACCUSE
Hacking Team viene accusata di lavorare per dittature ed è considerata tra i "nemici della Rete". Lunedì l'azienda subisce un attacco informatico: 400 giga di dati (mail, fatture ecc) trafugati

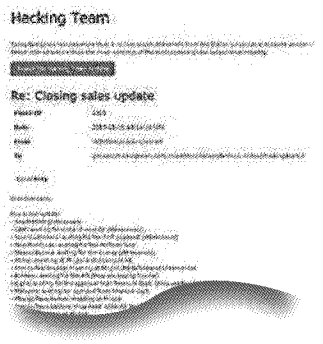
3

ISPEZIONE E WIKILEAKS
Il garante per la privacy ordina un'ispezione alla Hacking Team. In Rete si moltiplicano le polemiche su chi siano gli autori dell'attacco. Wikileaks pubblica un milione di mail


Hacking Team

Re: Re: Re: your proposal RCS (GALILEO)

GLI AFFARI CON IL SUDAN
"Dovremo dare seguito al nostro training e continuità alla tecnica di attacco". La mail che conferma il business col regime sudanese


Hacking Team

Re: Closing sales update

DAI SAUDITI ALLE FIAMME GIALLE
Un'altra delle email trafugate svela i clienti: dall'Arabia Saudita al Bahrein, dal Marocco alla Guardia di Finanza

Il Medio Credito Centrale aggiorna la scheda tecnica del fondo di garanzia per le pmi

Microcredito, controlli campione

Verifiche spot su beneficiari e operatori che erogano fondi

DI MARCO OTTAVIANO

Controlli a campione per il microcredito. Il gestore del fondo Pmi (e cioè il Medio credito centrale), in sede di verifica ovvero in sede di escussione, potrà effettuare verifiche sulla effettiva rispondenza dell'operazione del microcredito ai requisiti previsti dal decreto del ministero dell'economia e delle finanze n. 176/2014. In particolare le verifiche si soffermeranno sui soggetti beneficiari, sui parametri dell'operazione sulla somministrazione dei servizi ausiliari di assistenza e monitoraggio da parte dell'operatore di microcredito ovvero del soggetto terzo affidatario. Queste le nuove istruzioni contenute nella scheda tecnica sul microcredito del fondo di garanzia Pmi, elaborata dal gestore Medio Credito centrale e aggiornata a luglio.

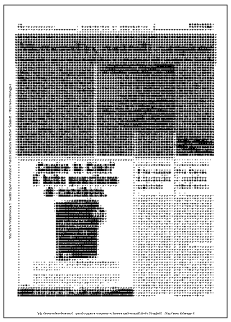
Servizi assistenza. L'intermediario finanziatore è tenuto a prestare, in fase istruttoria delle operazioni del microcredito e durante il periodo di rimborso, almeno due dei seguenti servizi ausiliari di assistenza e monitoraggio ai soggetti finanziati: supporto alla definizione della strategia di sviluppo del progetto finanziato e all'analisi di soluzioni per il miglioramento dello svolgimento dell'attività, formazione sulle tecniche di amministrazione dell'impresa, sotto il profilo della gestione contabile, della gestione finanziaria, della gestione del personale, formazione sull'uso delle tecnologie più avanzate per innalzare la produttività dell'attività, supporto alla definizione dei prezzi e delle strategie di vendita, con l'effettuazione di studi di mercato, supporto per la soluzione di problemi legali, fiscali e amministrativi e informazioni circa i relativi servizi disponibili sul mercato e supporto all'individuazione e diagnosi di eventuali criticità dell'implementazione del progetto finanziato. L'intermediario finanziatore può affidare, con contratto da stipularsi in forma scritta, i servizi ausiliari di assistenza e monitoraggio, a soggetti specializzati nella prestazione di tali attività. Il contratto deve prevedere, tra l'altro, l'obbligo di riferire periodicamente all'intermediario l'andamento delle attività svolte e i risultati conseguiti dai soggetti finanziati.

Finanziamenti. I finanziamenti non possono essere assistiti da garanzie reali e non possono eccedere il limite di euro 25 mila per ciascun beneficiario. Il limite può essere aumentato di euro 10 mila, qualora il contratto di finanziamento preveda l'erogazione frazionata subordinando i versamenti successivi al verificarsi delle seguenti condizioni: il pagamento puntuale di almeno le ultime sei rate pregresse e lo sviluppo del progetto finanziato, attestato dal raggiungimento di risultati intermedi stabiliti dal contratto e verificati dall'operatore di microcredito. L'intermediario finanziatore può concedere allo stesso soggetto un nuovo finanziamento per un ammontare, che sommato al debito residuo, non superi il limite di 25 mila euro o, nei casi previsti, di 35 mila euro. Il rimborso dei finanziamenti è regolato sulla base di un piano con rate aventi cadenza al massimo trimestrale. La data di inizio del pagamento delle rate può essere posposta per giustificate ragioni connesse con le caratteristiche del progetto finanziato.

Così i controlli

Verifica	Il gestore del fondo Pmi (e cioè il Medio Credito Centrale), in sede di controllo a campione ovvero in sede di escussione, potrà effettuare verifiche sulla effettiva rispondenza dell'operazione del microcredito ai requisiti previsti dal decreto Mef n. 176/2014
Oggetto delle verifiche	In particolare le verifiche si soffermeranno: - sui soggetti beneficiari; - sui parametri dell'operazione; - sulla somministrazione dei servizi ausiliari di assistenza e monitoraggio da parte dell'operatore di microcredito ovvero del soggetto terzo affidatario

IO La scheda tecnica sul sito www.italiaoggi.it/documenti



Il Campidoglio e le tracce di corruzione Così si arrivava agli appalti inquinati

Si dimette l'ex capo della segreteria di Marino. Gabrielli: con Alemanno Mafia Capitale intimidiva

L'indagine

di **Giovanni Bianconi**

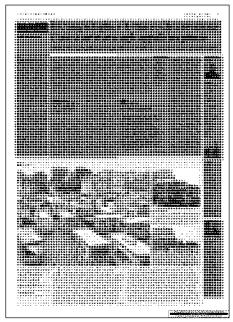
ROMA Ci sono piccole storie che svelano grandi irregolarità e sistematiche manovre corruttive, nelle pieghe dell'indagine amministrativa sulle infiltrazioni di Mafia Capitale nel Comune di Roma. Per esempio un appalto dal valore pressoché insignificante rispetto al «gigantismo» del bilancio generale (474.000 euro destinati alla gestione del servizio di pulizia e manutenzione degli arenili di Castel Porziano per il 2014), però emblematico del modo di operare della presunta associazione mafiosa guidata da Salvatore Buzzi e Massimo Carminati. Assegnato con una procedura in cui sono state rilevate diverse «carenze».

Il Comune aveva suddiviso l'appalto in due lotti, «per ognuno dei quali ha individuato i soggetti da invitare a gara; senonché tutti i soggetti invitati sono risultati direttamente o indirettamente riconducibili a Buzzi, alcuni addirittura parte integrante del suo sodalizio». Una ulteriore dimostrazione, secondo la commissione d'indagine, «dei collegamenti tra il sodalizio criminale e il vertice politico-amministrativo del Municipio». Nel caso specifico, quello di Ostia. Ma «il percorso amministrativo seguito da questo appalto si incrocia», per i commissari, con l'attività del Dipartimento Ambiente e Territorio del Comune sotto l'attuale gestione; in particolare con «l'atto di indirizzo adottato dall'assessore Estella Marino, su sollecitazione del dottor Altamura (dirigente arrestato per corruzione nella seconda fase dell'operazione della Procura, *ndr*) che ha innalzato l'importo degli appalti da riservarsi alle cooperative sociali».

Sempre a Ostia c'è la vicenda della nuova sede dei vigili urbani, «ospitati in un immobile di proprietà della Immobilgest, nonostante la metratura dei locali fosse inferiore a quella richiesta dal bando e la destinazione del bene non conforme»; il contratto è scaduto, ma l'amministrazione continua a pagare più di un milione all'anno come «indennità di occupazione». Quando il comandante della Polizia locale di Roma Raffele Clementi, «che in maniera a dir poco singolare non era stato affatto coinvolto nella procedura», lo venne casualmente a sapere, provò a opporsi. In maniera «ferma e formale». Inutilmente: «Il Dipartimento Patrimonio del Comune insiste nella volontà di stipulare il contratto a far data dal 1° aprile 2015». Il problema è che l'Immobilgest è «riconducibile alle proprietà di Mauro Balini», presidente del Porto di Ostia; un personaggio — scrivono gli ispettori — che con il suo corredo di relazioni e contatti è lo strumento attraverso cui l'organizzazione criminale effettua il salto di qualità verso attività commerciali di apparente rispettabilità e liceità».

La denuncia
Il prefetto: al contesto critico si aggiunge l'assenza di iniziative di organi esterni

I commissari concludono stigmatizzando «l'irregolarità della condotta del Comune nella gestione della gara», e anche questa considerazione è stata analizzata dal prefetto Gabrielli per arrivare alle sue determinazioni. Che da un lato hanno portato alla proposta dello scioglimento per mafia del Municipio di Ostia, dall'altro a utilizzare toni più indulgenti con l'assessore Estella Marino: «Non pare discutibile che il dottor Altamura sia inizialmente riuscito nell'intento di "orientare" l'assessore verso decisioni che riservavano alle cooperative una serie di affidamenti in materia di verde pubblico; ma è da sottolineare come ciò sia accaduto nei primi



I volti

Sindaco
Ignazio Marino, sindaco di Roma, finito nel vortice di Mafia Capitale. Tre Dipartimenti del Campidoglio su quindici sono risultati infiltrati dall'organizzazione criminale guidata da Massimo Carminati e Salvatore Buzzi per pilotare la politica cittadina

Prefetto
Franco Gabrielli, prefetto di Roma dal 2 aprile 2015. Gabrielli ha privilegiato la via della «discontinuità» della giunta Marino rispetto a quella guidata da Alemanno, indagato per mafia. Il prefetto ha ritenuto così di evitare il coinvolgimento dell'organo politico elettivo

tempi del suo incarico, quando è lecito ritenere che l'amministratore non avesse penetrato a sufficienza la conoscenza degli uffici a lei facenti capo, e dei personaggi che li popolavano».

Tra l'altro Gabrielli precisa che «alla criticità del contesto (ereditato dal sindaco Ignazio Marino dalla Giunta Alemanno, *ndr*) si aggiunge, duole dirlo, una generale assenza di iniziative di organi esterni capaci di fornire la dimensione del pericolo dell'infiltrazione mafiosa o, più in generale, delle anomalie esistenti nel sistema degli appalti capitolini; e questo nonostante che alcune rilevanti iniziative di indagine avevano portato alla luce significativi casi di malaffare riguardante le partecipate di Roma Capitale». Una censura apparentemente rivolta all'ex prefetto Pecoraro, il quale insediò la commissione d'accesso che ha riservato severe critiche non solo alla Giunta Alemanno ma anche a quella Marino.

Gabrielli ha concluso il suo lavoro proponendo, tra l'altro, la rimozione del segretario generale del Campidoglio in carica con entrambi i sindaci, Liborio Iudicello. Destinatario di analoga proposta era anche l'ex capo della segreteria del sindaco Marino, Mattia Stella, che nelle intercettazioni appariva come uno che Buzzi intendeva utilizzare per i suoi scopi. Stella ieri si è dimesso, (come Iudicello), e il sindaco gli ha ribadito vicinanza e solidarietà. Quanto alle due amministrazioni, il prefetto spiega che con Alemanno Mafia Capitale utilizzava «come strumento principe l'intimidazione mafiosa», mentre con Marino «la disponibilità di amministratori e dipendenti pubblici viene acquisita attraverso la corruzione».

36%

Gli appalti senza gare sul totale degli affidamenti del Campidoglio negli ultimi due anni di Alemanno

La parola

MAFIA CAPITALE

Mafia Capitale è una delle organizzazioni criminali di stampo mafioso-politico-affaristico che operava a Roma a partire dal 2000 condizionando le scelte dell'amministrazione della capitale.
A capo del sodalizio (37 gli arrestati) due pregiudicati: Massimo Carminati, già esponente del gruppo eversivo d'ispirazione neofascista Nuclei armati rivoluzionari e affiliato all'organizzazione malavitosa romana Banda della Magliana; e Salvatore Buzzi, bancario condannato a 20 anni per omicidio doloso e poi fondatore della Cooperativa 29 Giugno che si occupava di integrazione sociale.

Procuratore
Giuseppe Pignatone, procuratore capo di Roma. Nella relazione sull'operato della giunta Marino ha sottolineato come i tentativi di liberarsi di Mafia Capitale siano stati «molto parziali e scarsamente efficaci». Ma ha condiviso la linea di Gabrielli e la scelta di non sciogliere la giunta

Attacco informatico, l'allarme degli 007 Copiati codici delle reti di treni e energia

Il caso

di **Fiorenza Sarzanini**

ROMA L'attacco informatico contro la «Hacking Team srl» potrebbe mettere a rischio la sicurezza nazionale. Perché chi ha compiuto l'intrusione nel sistema non ha violato soltanto la segretezza del materiale custodito negli archivi dell'azienda, ma è riuscito a copiare anche i cosiddetti «codici sorgente». E questo potrebbe consentire l'intrusione nelle reti telematiche che governano le infrastrutture, da quelle ferroviarie, a quelle energetiche passando per la «protezione» di alcune postazioni strategiche. Non solo. Forze dell'ordine e servizi segreti collaboravano in maniera costante con la società milanese nella gestione di alcune attività investigative — in particolare per quanto riguarda le intercettazioni telefoniche, ambientali e dei computer — e questo sta causando conseguenze, anche gravissime, su numerose inchieste in corso.

Il blocco delle reti

C'è grande preoccupazione all'interno degli apparati per quello che è accaduto, ma soprattutto per quanto potrebbe succedere. La prima emergenza riguarda l'acquisizione dei dati custoditi legalmente dalla «Hacking» che vanta tra i suoi clienti principali la Telecom, ma anche altre enti di Stato. Il timore è che i «pirati» possano aver ottenuto informazioni preziose per bloccare alcune reti causando una paralisi del traffico. E possano decidere di agire a sorpresa. Palazzo Chigi assicura che sono stati messi in atto tutti gli interventi per «effettuare una nuova protezione», ma non viene negato che in questo momento sarebbe impossibile garantire sulla piena sicurezza anche perché le verifiche sono tuttora in corso e nessuno è ancora in grado di sapere se negli archivi dell'azienda ci fossero anche dati acquisiti illegalmente che potrebbero essere gestiti e utilizzati adesso da chi ha compiuto l'attacco. La polizia postale è al lavoro per ricostruire l'intrusione e cercare di individuare chi l'abbia compiuta, non escludendo che si tratti di qualcuno collegato a servizi segreti esteri, dunque a uno Stato «nemico». E lasciando anche aperta l'ipotesi che possa trattarsi di un vero e proprio atto terroristico. La possibilità che si tratti di qualcuno interno alla società viene ritenuta improbabile, così come l'eventualità di un'azione compiuta da un'azienda rivale.

L'attività degli 007

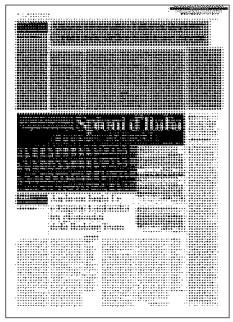
Le due agenzie di *intelligence* — Aisi e Aise — avevano un'attività comune con la «Hacking» e ciò rende ancor più complicata la situazione, perché l'inchiesta aperta dalla procura di Milano potrebbe anche portare a svelare alcune operazioni in corso che invece dovevano rimanere riservate. È possibile che — al di là del materiale pubblicato su internet — siano state acquisite informazioni ben più importanti e delicate che potrebbero essere utilizzate per scopi diversi da quelli apparenti che mirano a danneggiare gravemente l'azienda mostrando la sua vulnerabilità. Veri e propri ricatti, anche di altissimo livello, che potrebbero condizionare settori economici, finanziari e industriali. La convinzione di chi indaga è infatti che quanto avvenuto potesse avere un doppio obiettivo: smascherare l'attività della «Hacking» con alcuni Paesi ritenuti «canaglia» ma anche carpire informazioni che erano state ottenute grazie a questi contatti privilegiati.

Ricatti
È possibile che siano state acquisite informazioni sensibili Il rischio di ricatti

I dati personali

Gravi danni possono essere causati anche sulle inchieste in corso. Oltre al pericolo che vengano svelate le intercettazioni attivate per ordine della magistratura, esiste la possibilità che i dati sull'attività investigativa consentano ai pirati di utilizzare lo stesso sistema per avviare nuovi «ascolti» sulle utenze già sotto controllo, ma anche su quelle collegate. Con il rischio che vengano rubati i dati di migliaia di telefoni e computer. Potrebbero essere registrate conversazioni in voce e captati i messaggi sms, copiate le chat su Whatsapp e quelle via mail. Una violazione gravissima, dalle conseguenze imprevedibili.

fsarzanini@rcs.it

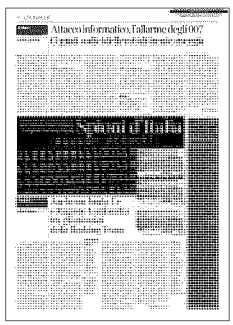


Oltreoceano

Quei dati rubati agli Stati Uniti web-vulnerabili

di **Giuseppe Sarcina**

Il gendarme americano si è appisolato sui computer. Mercoledì scorso amnesia collettiva, con il blocco informatico della United Airlines, dello Stock Exchange di New York e del *Wall street journal*. Ieri, invece, una notizia ufficiale: i pirati del web hanno rubato i dati di circa 21,5 milioni di cittadini entrati in contatto con gli uffici pubblici. Non solo: un altro gruppo di hacker si è impadronito dei file intestati a 4,2 milioni di impiegati e funzionari federali. Secondo le indiscrezioni pubblicate dal *New York Times*, le due incursioni sarebbero partite dalla Cina, anche se le autorità americane tacciono sul punto. La vulnerabilità delle reti è, però, a questo punto un dato incontrovertibile. Il capo dell'Fbi, James Comey, aggiunge regolarmente qualche particolare inquietante nelle sue audizioni al Congresso. Gli attacchi hanno già lambito il Dipartimento di Stato e la stessa Casa Bianca. Oppure hanno colpito le grandi multinazionali, aprendo un nuovo capitolo nella antica pratica dello spionaggio industriale. Su entrambi i fronti le contromisure sono in ritardo. Nel bilancio, alla voce «difesa cibernetica» sono stanziati 14 miliardi di dollari per il 2015 e 41,2 miliardi per il 2016. Evidentemente, lo sforzo finanziario non ha ancora prodotto risultati concreti. La diplomazia americana sta tentando di intensificare la collaborazione con gli alleati europei e l'Australia. Il presidente Barack Obama esita, invece, a porre la questione della sicurezza informatica sul tavolo dei rapporti bilaterali con la Cina e con la Russia. E si espone alle critiche dei repubblicani che pescano nell'inquietudine crescente dell'opinione pubblica.



la Repubblica

IL RETROSCENA / I SERVIZI SEGRETI: "ANCORA DA VERIFICARE L'IMPATTO SUI DATI SENSIBILI"

Svelati decine di obiettivi e contatti di intelligence: sicurezza italiana a rischio

CARLO BONINI

ROMA. Cosa è stato davvero compromesso della nostra sicurezza nazionale? E chi si nasconde dietro quell'avatar *"Phineas Fisher"* che promette di colpire ancora? Attivisti? Gruppi privati che lavorano per uno Stato? In un venerdì di luglio piuttosto complicato per i nostri apparati, la notizia è che alle domande chiave di questa storia di Hacking Team la nostra Intelligence non è in grado di rispondere con certezza. Che, dunque, e per dirla con il gergo degli addetti, il *damage assessment*, la stima del danno è ancora un dato volatile come le risposte balbettate in queste ore dalla società milanese di fronte alle sollecitazioni dei nostri Servizi.

«Neanche loro sono in grado di stabilire con esattezza fin dove è arrivata l'intrusione - spiega una fonte qualificata della nostra Intelligence - E questo è un grosso problema. Non sanno quanti codici sorgente dei loro software spyware che noi usavamo sono stati hackerati. E dunque, a nostra volta, noi non siamo in grado, in questo momento, di stabilire se chi ha rubato quei dati sia nelle condizioni di ricostruire quando, in che modo e contro chi abbiamo usato quei software. Il che significa che non possiamo escludere che chi ha messo le mani su quei dati sia in grado di tracciare alcuni degli obiettivi del nostro spionaggio all'estero o, peggio, anche le informazioni che sono state raccolte durante quel tipo di operazioni».

Delle nostre due Agenzie, la faccenda riguarda l'Aise, il nostro spionaggio all'estero. Perché è lei che, da qualche anno, utilizzava i prodotti di controllo remoto (Rcs) brevettate dalla società di via Moscova. «Diciamo pure con franchezza - prosegue la fonte - al netto di quello che Hacking team riuscirà a ricostruire, che diamo per scontato che almeno i nostri "obiettivi" lavorati con quei software siano stati compromessi. Parliamo di qualche decina di target. Tutti all'estero. E per lo più legati a operazioni di intelligence economica e di ricostruzione dei flussi finanziari di sostegno al terrorismo islamista». Quanto ai dati di intelligence raccolti con quei software, «speriamo nello stellone italiano», conclude la fonte.

L'allarme ai nostri Servizi è arrivato dieci giorni fa. E da quel momento i sistemi di controllo remoto prodotti da Hacking Team in uso al nostro spionaggio estero sono stati "spenti" e svuotati dei loro database per essere messi al sicuro. Tuttavia, se la mossa sia stata o meno tempestiva nessuno può giurarlo. Perché nessuno è in grado di stabilire quando l'effrazione informatica sia cominciata davvero. Quando, cioé, abbia avuto inizio il travaso di dati e codici sorgente. Probabilmente - questa l'ipotesi accreditata dalla nostra Intelligence - molto tempo prima che scattasse l'allarme. E con modalità che lascerebbero intuire un "furto" dalle stimmate diverse di quelle di un classico attacco hacker. O, quantomeno, un furto che dell'attacco hacker doveva avere le sembianze per poter allontanare il sospetto di un'operazione più raffinata e insidiosa.

È un fatto che il milione di documenti (per lo più, comunicazioni interne all'azienda e mail scambiate con la sua clientela di Governi, Servizi e Polizie di mezzo mondo) scaricati in Rete, appaiano, nell'ottica di chi di mestiere fa lo spionaggio e dunque ritiene che «non sia mai vero ciò che appare tale», né più e né meno che un "ballon d'essai". «Un'esca». «Polvere gettata negli occhi delle opinioni pubbliche mondiali per distogliere l'attenzione dal vero obiettivo del furto informatico». La divisione Informatica dell'Aise da giorni sta raccogliendo in rete quei documenti (parzialmente diffusi da WikiLeaks), analizzandoli con una stringa di ricerca in grado di stabilire i nomi di quali agenti, operazioni o informazioni classificate siano andati bruciati. E i primi risultati parlano di una evidente sproporzione tra informazioni politicamente sensibili (come quelle relative alla vendita di spyware a dittature e regimi impegnati nella repressione delle libertà civili) e informazioni classificate riguardanti la sicurezza nazionale.

Una buona notizia, a ben vedere. E, tuttavia, tale solo se vista appunto con occhi sgombri dalla paranoia professionale di chi non può per mestiere accontentarsi della prima evidenza. Come dimostra la fretta con cui, nelle ultime 24 ore, è stata verificata e smentita dal Dis (il vertice dei nostri Servizi) una delle informazioni contenuta in una di quel milione di mail: la presenza contemporanea, nel febbraio scorso, ad Abu Dhabi per la fiera degli armamenti, del ministro della Difesa Pinotti e del direttore dell'Aise Manenti. «Il fatto che quella informazione, per altro di per sé neutra, sia solo in parte vera - osserva una fonte del Servizio - è motivo di qualche preoccupazione. Perché ora abbiamo anche un'altra domanda a cui rispondere: chi giocava a manipolare le informazioni dentro Hacking team o con Hacking team? E perché?».


L'inchiesta
I segreti bruciati di Hacking Team
Svelati decine di obiettivi e contatti di intelligence: Sicurezza italiana a rischio


"Palazzo Chigi fece pressioni per noi"

la Repubblica

REGOLE E CLIENTI (CINESI)

FABIO CHIUSI

Lo scandalo Hacking Team è una questione seria e complessa. Seria perché ci sono di mezzo la sicurezza nazionale, i diritti umani, i limiti del controllo in Rete e di tecnologie che, nate per aiutare le forze dell'ordine, si scoprono usate contro dissidenti, giornalisti in Paesi non democratici.

Complessa perché sono ancora ignoti movente e identità dell'attaccante. Conosciamo solo un nome su Twitter, *Phineas Fisher*, e la sua minaccia di colpire ancora. Ma chi è *Phineas Fisher*? Davvero si tratta dello stesso hacker, o gruppo di hacker, che l'anno scorso rivendicò il furto dei dati di Gamma International, altra grande compagnia internazionale di sorveglianza tech? La pubblicazione indiscriminata del materiale prelevato all'azienda milanese significa che insieme a informazioni di chiaro interesse pubblico — le fatture per i servizi sostenuti per il Sudan — circolano ora non solo dati sensibili che avrebbero dovuto restare riservati, ma anche il codice sorgente dei suoi *spyware*. Con ciò che ne consegue per la sicurezza dei suoi clienti, e l'integrità delle indagini svolte attraverso il loro utilizzo.

La prima impressione è che dietro lo scandalo sia in corso uno scontro frontale tra chi vuole provare a parare il colpo e chi vorrebbe che l'azienda sparisse. Di certo la strategia utilizzata da Hacking Team nei 5 anni in cui i critici le hanno posto domande precise circa i suoi clienti — non confermare né smentire, ma tacere — non ha aiutato. Ma è anche vero che se quel materiale, finito ora su Wikileaks, avesse passato il vaglio del filtro giornalistico, come è successo con l'archivio Snowden, l'impressione di un'operazione nel puro interesse del pubblico sarebbe stata più forte — e quella di una vendetta più debole.

Resta, comunque vada a finire, il problema di come regolamentare l'industria dei produttori di strumenti digitali di sorveglianza. Mercato miliardario che conta un centinaio di soggetti tutt'altro che trasparenti, e per le cui regole sono in arrivo ipotesi di modifica che negli Usa hanno già diviso la comunità della *cybersecurity*.

L'intesa che si intende emendare, il cosiddetto accordo di Wassenaar, è volontaria. E se anche si approvassero norme più stringenti per le aziende occidentali, potrebbero restare scoperte le altre. Con il rischio di una migrazione dei clienti più problematici verso le tecnologie di Paesi meno controllabili, Cina in testa. Insomma, la partita è aperta; il risultato, tutt'altro che scontato.


"Palazzo Chigi fece pressioni per noi"