

Rassegna del 12/01/2017

POLITICA INTERNA

SOLE 24 ORE IL PIN UNICO RAGGIUNGE QUOTA UN MILIONE 1

GIUSTIZIA

SOLE 24 ORE PASSWORD, SITI E BANNER TRUFFA: LE MOSSE PER *B.SIM.* 2
RESPINGERE L'ATTACCO

MESSAGGERO SICUREZZA, LA DIFFERENZA LA FANNO I FONDI «GLI *VENTURA MARCO* 3
USA 87 MILIARDI, NOI 250 MILIONI»

IL FATTO DA BALZAC A SUN TZU FINO A GELLI IL *D'ESPOSITO* 5
QUOTIDIANO DOSSIERAGGIO È SEMPRE POTERE *FABRIZIO*

LA GIORNATA

PUBBLICA AMMINISTRAZIONE

Il pin unico raggiunge quota un milione

■ Il Pin unico, nome ufficiale Spid, sembra avere ingranato: le identità digitali, per accedere con una sola password ai servizi online della P.a. «hanno raggiunto 1 milione». Lo ha annunciato ieri il ministero della Pubblica Amministrazione, spiegando che il numero delle password rilasciate ha registrato una svolta in parallelo con «la crescita del numero dei servizi disponibili». E, ha sottolineato il ministero, «da lunedì 16 gennaio con le credenziali Spid sarà possibile accedere al servizio online del Miur per l'iscrizione dei propri figli alle prime classi delle scuole primarie e secondarie di primo e secondo grado per l'anno scolastico 2017-2018». Chi avrà Spid «non dovrà più registrarsi ogni anno, come invece avviene per chi utilizza soltanto il servizio online del Miur». Intanto il rialzo fin qui rilevato stando ai dati dell'Agid è, si evidenzia, «per gran parte riconducibile all'attivazione dei servizi App 18 (bonus-cultura per i diciottenni) e Carta del docente per l'aggiornamento professionale». Solo nell'ultima settimana «le identità digitali rilasciate dai quattro identity provider sono state 70 mila». In realtà la progressione è iniziata da novembre, proprio grazie a bonus cultura e quello per i prof. Inoltre «dai primi mesi di quest'anno, oltre ai 4.273 servizi già disponibili da parte di 3.720 amministrazioni pubbliche, sarà possibile con Spid richiedere l'anticipo finanziario a garanzia pensionistica (Ape)».

© RIPRODUZIONE RISERVATA



La vulnerabilità digitale. Attenzione alle estensioni dei file malevoli e protezione con il second checking

Password, siti e banner truffa: le mosse per respingere l'attacco

IMPRESE E PROFESSIONISTI

Spesso vittime sono le aziende e gli studi professionali. Per questo è necessario aggiornare costantemente i software

■ Se fino a ieri il grande incubo era la Nsa americana e la sua vasta rete di spioni, l'operazione Eye Pyramid ci ha detto una verità tutta nuova: non servono grandi agenzie, né investimenti ingenti per captare le comunicazioni informatiche di politici, istituzioni e professionisti. Basta un malware e qualche riga di codice per trafugare 18.327 username, 1.793 password e oltre 87 giga byte di dati sensibili. Questi numeri - che sono quelli dell'operazione che ha incastrato i fratelli Occhionero - aprono il campo a una serie di interrogativi.

Come difendersi

Abbiamo già scritto ieri che Eye Pyramid è un malware ben fatto, invisibile agli antivirus più diffusi grazie a sistemi di codifica molto intelligenti. Ciononostante la sua struttura di propagazione è abbastanza banale, e rimanere impigliato nella sua rete non è proprio semplice. Aprire una mail contenente un malware, infatti, non determina l'infezione del proprio computer. Il rischio sta tutto nell'allegato, o nel contenuto dell'email. Il primo passo da fare, dunque, è quello di valutare attentamente la provenienza e il contenuto della email prima di aprire un allegato o di cliccare su un link contenuto all'interno della mail stessa. I malware si installano esclusivamente dopo una di queste operazioni. Per difendersi da Eye Pyramid, dunque, bastava semplicemente non cliccare l'allegato. Solitamente gli allegati malevoli hanno estensioni: fare attenzione alle estensioni dei file prima di aprirli. Quelli potenzialmente pericolosi includono le estensio-

ni .exe, .hta, .wsf e .js.

Cambiare password

Utilizzare una password e per molto tempo è una delle vulnerabilità digitali più diffuse. La pigrizia è un cattivo alleato, in questo senso. Cambiare le password con frequenza non ci mette certo al riparo da attacchi informatici, ma è una buona forma di difesa.

Mai password uguali

La vita digitale di ognuno di noi, troppo spesso, è fatta di una sola password. La utilizziamo per accedere alle caselle di posta, ai social, al servizio di cloud. Ed è così che diamo una grossa mano agli hacker. Perché gli basta una sola password per fare bingo sull'intera vita digitale di un utente. Utilizzare password diverse per ogni account è una buona abitudine. In questo senso, l'esempio di Yahoo! è lampante. La società californiana ha confermato, in queste settimane, che dal 2013 al 2014 sono stati trafugati i dati un miliardo e mezzo di account dai loro server. Molti di quegli utenti non utilizzano più Yahoo!, ma utilizzano ancora quella password per i loro account attivi. Le conclusioni sono ovvie.

Attivare il second checking

È una novità introdotta da molti servizi solo negli ultimi tempi. E porta numerosi benefici. Quella di attivare il second checking per gli account in nostro possesso è sicuramente una buona abitudine. Si tratta di uno strumento utile a prescindere dall'account per il quale lo si usa (posta elettronica, dropbox, di iCloud, social network). Un second checking può essere determinante per tenere fuori gli spioni. Alcuni servizi consentono di attivarlo anche attraverso un sms con un codice identificativo e temporaneo che arriva sullo smartphone e senza il quale è impossibile accedere.

Sistemi sempre aggiornati

Eye Pyramid riusciva ad infettare solamente macchine con sistema operativo Windows, e - come detto - era invisibile agli antivirus più comuni. Tuttavia, aggiornare costantemente software (antivirus ma anche il proprio browser di navigazione e il pacchetto office) e sistema operativo è un consiglio sempre utile. Occhio però a non usare due antivirus contemporaneamente, potrebbero entrare in conflitto.

Siti e banner truffa

Un malware può essere diffuso attraverso tecniche di phishing (e cioè tramite l'invio di una mail), ma anche tramite un sito Internet. Per questo è necessario prestare estrema attenzione. Navigare sempre su siti sicuri (quelli che hanno protocollo sicuro https) e non cliccare su banner pubblicitari esca sono accortezze fondamentali. Inoltre, è meglio fare attenzione ai contenuti espliciti (spesso a sfondo sessuale).

Studi e aziende

Molto spesso le vittime di attacchi malware - e ultimamente soprattutto ransomware - sono le aziende e gli studi professionali. Per questo è necessario "educare" gli impiegati dell'azienda, aggiornare costantemente i software sui computer aziendali, condurre regolarmente verifiche di sicurezza e analizzare le email che provengono da mittenti sconosciuti.

B.Sim.

© RIPRODUZIONE RISERVATA



Sicurezza, la differenza la fanno i fondi «Gli Usa 87 miliardi, noi 250 milioni»

GLI ESPERTI: GUERRA DA COMBATTERE CON GLI INVESTIMENTI «LE PORTE BLINDATE COSTANO, MA BISOGNA FARLE»

IL FOCUS

ROMA «I capi di governo sono come noi. Siamo tutti infestati di pin e password che non ricordiamo e alla fine scegliamo quelle più facili. Invece di doppi slash, punti interrogativi e asterischi, il nome di nostra figlia o del cane. Questa è la verità». Per Alfredo Mantici, direttore di Outlook News già capo degli analisti del Sids (il servizio di sicurezza interno) il tallone d'Achille di vip e comuni mortali è questo. Angela Merkel, per esempio. Aveva 3 cellulari 2 dei quali criptati, inaccessibili grazie alle tecnologie degli 007 tedeschi. Il terzo era un telefonino tradizionale e su quello le sue conversazioni sono state violate.

GLI AMERICANI

Americani spioni, tedeschi a loro volta spioni di Kerry e della Clinton. Già, Hillary. Che ha dovuto dire addio alla Casa Bianca per la sua imprudenza informatica. «Utilizzò la sua mailbox personale e tutta una serie di mail vennero trafugate», sottolinea Roberto Baldoni, direttore del Centro di Cyber Intelli-

gence e Information Security dell'Università di Roma "La Sapienza". «Eppure, i servizi nei loro rapporti le avevano raccomandato di usare un certo tipo di applicativi. Dobbiamo immaginare il numero di mail e telefonate di un politico di livello, che per non perdere tempo sceglie alla fine la soluzione semplice. La cultura della sicurezza deve nascere in ognuno di noi. Tanto più che il tipo di attacco che è stato fatto non era particolarmente sofisticato». Il fattore umano «è fondamentale» per il generale della Guardia di Finanza Umberto Rapetto, già comandante del Gruppo anticrimine tecnologico. Nel 2001 catturò e fece condannare gli hacker entrati nei siti del Pentagono e della NASA. «Proprio la scarsa cultura in materia, la non consapevolezza del pericolo informatico, la ridotta adattabilità a regole e precauzioni, e l'incapacità di ammettere la propria ignoranza, sono i punti deboli - dice Rapetto - del bersaglio dei pirati informatici o anche di hacker balordi improvvisati». Chi è abituato «a segreterie, anticamere e scorte armate crede di poter contare su una schermatura naturale. I filtri del vivere quotidiano non attecchiscono nel contesto digitale».

I POTENTI

I potenti sono uguali a tutti gli altri «davanti a smartphone, tablet e computer, basta con un clic improvvido aprire una mail con un al-

legato 'velenoso' e in un attimo il malware entra in azione senza rispetto per il rango sociale o il ruolo istituzionale di chi possiede l'apparato». Altro elemento decisivo è la sorpresa. Rapetto: «Come a scacchi, è in vantaggio il bianco, chi muove per primo. Chi attacca ha ottime probabilità di riuscita». Il fatto è che «la protezione dovrebbe essere indipendente dalla volontà del vip - insiste Mantici - e nella sicurezza bisogna investire. Nel bilancio 2015 della NSA americana c'erano 87 miliardi di dollari. In Italia ci siamo impiccati per 250 milioni per la cyber security istituzionale. Un esperto di sicurezza amico di Renzi come Carrai aveva ragione: lui, amico degli israeliani, sapeva benissimo che abbiamo una casa piena di tesori, protetta da una porta di vetro. La sicurezza è un bene immateriale, capisci quanto vale quando ti entrano i ladri in casa. Le porte blindate costano, ma vanno fatte». A Radio24 Giuliano Tavaroli, ex capo della sicurezza Telecom e Pirelli, ha ricordato l'annuncio francese un mese fa di investimenti da 1 miliardo e 400 milioni di euro per la cyberwar, e i britannici 15 miliardi di sterline, «mentre noi questa guerra la stiamo perdendo per scarsità di risorse». Monito finale per vip e gente comune da Baldoni: «I software sui dispositivi devono essere sempre aggiornati, perché le nuove versioni includono la chiusura delle falle del sistema».

Marco Ventura

© RIPRODUZIONE RISERVATA



Il parere

«Impossibile decriptare gli atti senza password»

La decriptazione del materiale raccolto dai fratelli Occhionero, «è difficile se non impossibile», serve la password. È questa l'opinione di Matteo Flora, informatico ed esperto di sicurezza. «I dati memorizzati sono sia su server statunitensi sia su server cloud dove sembra che Occhionero avesse il materiale più corposo - aggiunge -. Decifrare il suo lavoro è praticamente impossibile, ci vogliono una password e un algoritmo potente, romperli con la forza bruta è difficile». C'è una possibilità, «se gli inquirenti nel sequestro hanno portato via il codice sorgente del malware impiegato per infettare i computer da lì si può risalire alla password che serve anche per il materiale negli Usa»

Come difendersi dai pirati del web

- 1** Attenzione a mail e chat sui social: il mittente è un nome conosciuto, ma il testo ha parole strane
- 2** Verificate sempre gli Ip e non fate home banking su un computer su cui si scarica qualsiasi altra cosa
- 3** Aggiornate continuamente gli antivirus. Anche quelli sui telefonini



QUELLA STORIA D'ITALIA
RISCRITTA DAI DOSSIER

◉ FABRIZIO D'ESPOSITO A PAG. 6

RICATTI La Repubblica delle P (2,3,4...)

Abitudini

Da Balzac a Sun Tzu fino a Gelli Il dossieraggio è sempre potere

Usare i segreti di chi comanda è un gioco antico quanto la politica: brevestoria dello "chantage"

Dietro le trame

Agenti dei servizi, carabinieri e spioni semplici: il catalogo dei professionisti

Iipse dixit



LICIO
GELLI

La P2 era un'associazione seria e massonica con sei ministri, un'ottantina di generali, il mondo dell'economia e dell'editoria



GIULIO
ANDREOTTI

Se vuole consultare il mio archivio glielo faccio vedere. Non ho mai ritenuto che il potere consistesse nel farsi i fascicoli per ricattare

FABRIZIO D'ESPOSITO

Il grande Balzac definì il dossieraggio con un termine quasi frivolo. "Chantage", che nelle *Illusioni perdute* del 1839 viene presentato come "un'invenzione della stampa inglese, importato recentemente in Francia". Spiega Étienne Lousteau a Lucien de Rubempré: "Lo chanteur (cantante, ndr) si è procurato qualche pezza d'appoggio, qualche documento importante, così chiede un appuntamento all'arricchito di cui i documenti parlano. Se il tipo non dà subito una qualche somma, lo chanteur gli mostra come la stampa sia pronta a iniziare una campagna contro di lui, a rivelare i suoi segreti. L'uomo ricco ha paura, e paga. Il gioco è fatto". Nella Russia di Putin, invece, si chiama "kompromat" il sistema per ricattare o chiedere fedeltà con "particolari" documenti.

DA SEMPRE la conoscenza genera potere. Meglio, la conoscenza è il potere stesso. E l'af-

faire Occhionero, un cognome perfetto per un torbido noir di spioni, aggiunge un altro capitolo all'infinita storia segreta dell'Italia, che resta pur sempre la repubblica di Machiavelli, erede di quel Sun Tzu che nel suo celebratissimo *L'arte della guerra* sentenziò che "un esercito senza agenti segreti è esattamente come un uomo senza occhi né orecchie". La questione atavica, allora, è l'uso di quel che captano occhi e orecchie. I 18 mila nickname dei fratelli Occhionero rimandano per esempio al Grande Orecchio alias lo scandalo Tavaroli, dal nome del capo della security di Telecom che nel primo decennio del duemila assemblò intercettazioni e dossier, per un totale di oltre 40 mila parti lese. Nell'archivio segreto c'era di tutto, da Calciopoli al presunto patto occulto tra Bossi e Berlusconi, ossia

70 miliardi di lire che l'ex Cavaliere avrebbe versato per garantirsi la fedeltà assoluta della Lega.

In un mondo senza più confini grazie alle infinite connessioni del web, l'ultima frontiera dello spionaggio è introdursi nei pc che contano. Nel gennaio di due anni fa, sempre a Roma, fu arrestato un commercialista di nome Paolo Oliverio, che aveva accumulato fascicoli carpando informazioni con un software denominato "spyphone". Altri nomi eccellenti, altri vip. Altri ricatti. Hacker o malware o virus, l'importante è spiare. Questa nuova strada venne già scoperta dai pm di Napoli che



indagarono sulla P4 di Alfonso Papa, ex deputato berlusconiano, e del faccendiere pregiudicato Luigi Bisignani.

Qui si entra nel pieno delle faide politiche e della tenuta di uno Stato democratico. Spesso, infatti, i dossier servono a costruire equilibrio e egemonie all'interno delle istituzioni. Nelle indagini sulla P3 di Carboni e Verdini ci fu un politico reo confesso che ammise di aver confezionato un falso dossier su Stefano Caldoro, poi eletto governatore della Campania. A commissio-

narlo, secondo questa ricostruzione, sarebbe stato Nicola Cosentino, oggi sotto proces-

so per camorra. L'episodio va ricordato perché si basa su un'antica specialità settecentesca del ricatto: le accuse di omosessualità.

NELLA PRIMA Repubblica del regime democristiano, lo Stato parallelo ha due pilastri reazionari, filoatlantisti e anticomunisti. Il primo è il Piano Solo, ancora oggi un mistero in divenire, con continue rivelazioni. Questi i fatti. Era il 1964. Antonio Segni, presidente della Repubblica, e il generale Giovanni De Lorenzo, comandante dei carabinieri, erano preoccupati per "il salto nel buio" del centrosinistra perseguito dal leader dc Aldo Moro. Il golpe poteva essere una drammatica via d'uscita. De Lorenzo era uno degli uomini più potenti grazie alla "conoscenza" incamerata da capo del Sifar, i servizi segreti militari. Il Piano Solo prevedeva "l'enucleazione" di 700 personaggi vicini al Pci, tutti schedati e spiati. Lo spettro di un colpo di Stato ritornò sei anni dopo, nel 1970, con il fallito golpe Borghese: fu Giulio Andreotti nel 1974 a cancellare i fascicoli con i nomi dei militari massoni coinvolti.

IL SECONDO pilastro dello Stato parallelo, tra dossier e ricatti, è la famigerata P2 di Licio Gelli, la loggia "coperta" cresciuta nel Grande Oriente d'Italia, la maggiore obbedienza

massonica del nostro Paese (la stessa cui è iscritto il fratello Occhionero, subito sospeso dal gran maestro Bisi). Nell'elenco segreto gelliano, scoperto nel 1981, c'era anche il nome di Silvio Berlusconi, e finanche un progetto politico chiamato "Piano di rinascita democratica". Per la commissione d'inchiesta parlamentare di Tina Anselmi fu "un'organizzazione criminale". Quando trent'anni dopo, nel 2010, i magistrati diedero il nome di P3 alla loggia paramassonica di matrice berlusconiana, ecco cosa disse il venerabile Gelli: "Potrei anche offendermi. Come si fa a paragonare un'associazione massonica e seria com'era la P2 a un sodalizio tra affaristi, finalizzato solo a fare soldi. Noi si aveva sei ministri, un'ottantina di generali, il mondo dell'economia e dell'editoria. Tutti legati da un'idealità: fare il bene del Paese". I segreti di Gelli, morto nel dicembre del 2015, sono appaiati a quelli di Giulio Andreotti, presunto Grande Vecchio dello Stato parallelo, che a Oriana Fallaci confessò: "Se vuole consultare il mio archivio glielo faccio vedere. Non ho mai ritenuto che il potere consistesse nel farsi i fascicoli per ricattare".

NELL'ITALIA berlusconiana del ventennio breve, la Seconda Repubblica, la pratica del dossieraggio ha avuto un'inquietante "liberalizzazione". Clamorosa la rete messa su da Pio Pompa, agente del Sismi di Pollari, con l'obiettivo preciso di "disarticolare l'opposizione di sinistra". Del resto, contro l'Ulivo prodiano o il centrosinistra dalemiano c'è stato il festival delle bufale o degli sbiancamenti, dall'improbabile Igor Marini dell'affare Telekom Serbia (nome in codice di Prodi: "Mortadella") alle rivelazioni parziali sul dossier Mitrokhin, le spie al servizio dei sovietici (chi era il ministro ulivista spione?).

La storia delle trame segrete continuerà anche dopo i fratelli Occhionero, non c'è dubbio.

È lo "chantage", bellezza.

© RIPRODUZIONE RISERVATA