CYBER-ANTISEC 2019

REPORT DI SICUREZZA

PERIODO 2012-2018

Documento redatto da Edoardo Limone
edoardo@edoardolimone.com

Sommario

Generalità *3*

Sugli attacchi del periodo 2012-2018 ..... *4*

Gli hacker *6*

Categorie rilevate *10*

Politica **11**

Ambiente **11**

Sanità **11**

Attacchi: tipologie e modalità *13*

In merito alle cause dei breach **15**

Hacking Istituzionale: testare la debolezza dello Stato **16**

Principali aspetti di criticità *17*

Adozione delle password **17**

Tempi di reazione molto lenti e non sempre adeguati **17**

Carenza di comunicazione e di organizzazione **18**

Conclusioni *20*

Indice delle figure

Figura 1 - Arta Abruzzo è il primo bersaglio del 2018 5

Figura 2 - La testata del canale Twitter della LulzSec_ITA 6

Figura 3 - Il logo della LulzSec_ITA 7

Figura 4 - Il logo di Anonymous Italia 7

Figura 5 - Mappa degli hacker censiti 9

Figura 6 - Un esempio di defacing ai danni dell'Accademia Italiana Privacy 13

Figura 7 - Defacing del 27/11/2019 18

Figura 8 - Defacing del 28/11/2019 18

Generalità

Dal 2012 l'Italia riceve un numero crescente di attacchi hacker di varia natura; ci sono attacchi con finalità politica, di lucro, di danneggiamento. Tenerne traccia è assai difficile data l'eterogeneità delle sorgenti, dei mezzi usati per il contagio (vettori) e degli obiettivi (target).

Alcuni organismi italiani hanno provveduto a mettere assieme dati provenienti da più fonti, con lo scopo di creare uno scenario analitico più completo possibile. D'altro canto, c'era necessità di analizzare a fondo la tendenza di crescita di alcune tipologie di cyber attacco poiché dal 2012 ad oggi l'hacking ha subito un forte mutamento.

Da fenomeno prettamente tecnico, dimostrante la preparazione tecnica degli attaccanti, è mutato in una forma di fenomeno sociale con l'intenzione di incarnare gran parte del malcontento della popolazione. È stato trasformato dagli hacker stessi, in un certo senso, in una forma di "scudo" contro le ingiustizie dello Stato. Un esempio tra tutti sono le *operations* di Anonymous, intenzionate a denunciare le negligenze, gli abusi e gli illeciti della macchina statale seppur con mezzi illeciti.

Oggi l'hacking è diventato qualcosa a cui ci stiamo lentamente abituando ma, per chi lo studia, sta diventando anche un fenomeno di "stress" delle leggi nazionali ed europee, prima tra tutte il GDPR. Per gli hacker la continua normazione senza la corretta divulgazione della cultura della sicurezza e l'applicazione delle sanzioni previste, è semplicemente inutile. Per dimostrarlo sono stati compiuti numerosi attacchi nell'autunno del 2018 e tutti finalizzati a stressare il GDPR e i meccanismi di segnalazione.

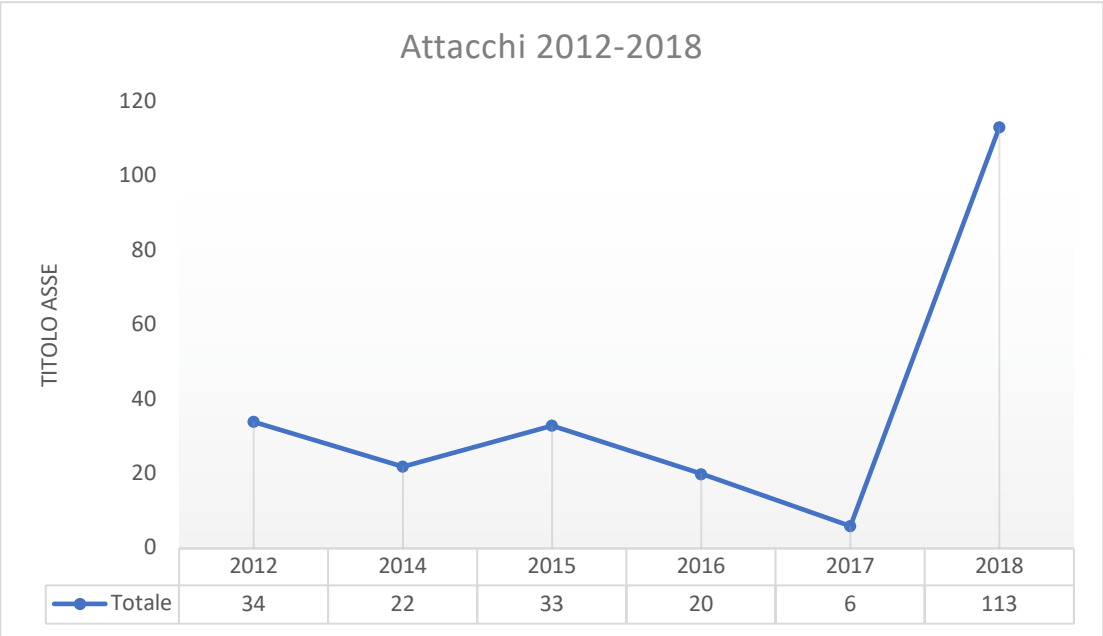
Con il presente documento si fornisce uno spaccato circa i dati raccolti, offrendo un'analisi sia qualitativa che quantitativa, basata su mesi di studi e di confronto con altri analisti di sicurezza. In questa prima versione del "Cyber AntiSec Report", si è cercato quindi di mettere a sistema la molteplicità di dati raccolti. È mio più profondo auspicio sperare che questo documento possa essere di aiuto ai lettori per comprendere meglio un fenomeno crescente e di fondamentale importanza per chi vuole intraprendere una professione nel digitale.

Edoardo Limone

Sugli attacchi del periodo 2012-2018

Gli attacchi oggetto di censimento sono quelli di cui è stata data evidenza sugli organi di stampa o sui siti web, con un sufficiente livello informativo da poter classificare l'azione offensiva all'interno di un'apposita scheda che, nel tempo, è cresciuta. Sono stati esclusi quindi gli attacchi provenienti dalle email, contenenti allegati malevoli, perché le informazioni fornite non erano sufficienti per creare un profilo adeguato dell'attacco e dell'attaccante.

Ci si è concentrati maggiormente sulle attività del gruppo Anonymous Italia ma anche su quelle di gruppi differenti come AnonPlus e altri ancora.



Dal 2012 al 2018 oggi sono stati identificati e censiti 228 attacchi ed è opportuno notare il declino che si è verificato dal 2015 al 2017 e rapida crescita tra il 2017 e il 2018. Questo trend aveva portato inizialmente portato a ritenere l'hacking organizzato non fosse problematico, ma dal 2018 il numero degli attacchi è così tanto aumentato quasi da superare in soli dodici mesi quelli di tutti gli anni precedenti.

Ma che cosa ha scatenato un numero così elevato di attacchi? Sono le *operation* che portano alla ribalta il gruppo Anonymous e la prima è quella che attesta un data breach con defacing fatta ai danni di Arta Abruzzo.

Figura 1 - Arta Abruzzo è il primo bersaglio del 2018

Fino a quel momento l'attività si era tenuta su un profilo molto basso. Sì, c'era stata la denuncia di un paio di siti che pubblicavano materiale pedopornografico ma è con Arta Abruzzo che inizia la raffica di data breach e defacing. Da questa data il gruppo Anonymous sembra aver preso una nuova vita portando attacchi di caratura più elevata e con una frequenza mai vista prima di quel momento.

Per capire cosa sia successo è fondamentale guardare l'attività del gruppo senza alcun pregiudizio ma avere una lente critica. Nel 2018 inizia un potente processo di "svecchiamento" dell'organizzazione italiana di Anonymous, con un avvicinamento del gruppo al sociale. Gli hacker sembrano voler far sentire la loro presenza e la comunicazione si fa così tanto poliedrica da riuscire a catturare una grande quantità di pubblico, eterogeneo per età e tipologia.

I temi sociali, già ampiamente cavalcati dai giornali e resi spesso silenti dalla politica, vengono quindi accolti bene dai cittadini e cominciano ad avere una certa cassa di risonanza sui social (Twitter e Facebook in particolare), andando ad incuriosire anche chi, prima di quel momento, non aveva capito chi fosse Anonymous.

Basti pensare che il 12 febbraio 2018 l'iniziativa contro la pedofilia non aveva raccolto praticamente nessun commento (solo 1 e non di discussione), mentre il 16 aprile 2018 l'attacco al sito artaabruzzo.it ne ha raccolti 4 di cui 2 di ringraziamento. È così che inizia una rapida escalation verso una forma di hacking che potremmo definire *hacking sociale*.

L'attività del gruppo si frappone tra quella istituzionale dello Stato e quella dei cittadini e quando a loro giudizio non vi è trasparenza nelle azioni, interviene attraverso data breach accompagnati spesso da defacing.

Gli hacker

È più difficile riuscire a distinguere i reali autori degli attacchi perché, anche se riportati sui canali ufficiali, vi è una collaborazione molto stretta tra le varie frange del gruppo. In questi anni la mia attenzione si è focalizzata sul gruppo LulzSec_ITA, responsabile di una delle più importanti azioni di comunicazioni fatte per Anonymous.

Figura 2 - La testata del canale Twitter della LulzSec_ITA

L'attività svolta dalla LulzSec è stata quella di rinnovamento (o per meglio dire svecchiamento) dei messaggi, facendo uscire Anonymous da uno stile troppo luttuoso

(sfondi neri con caratteri bianchi) e dando una linfa completamente nuova al modo di comunicare. Colori, emoticons, meme, sono tutti elementi grafici che entrano a far parte delle comunicazioni ufficiali, in un'esplosione di colori ed in un tripudio di comicità ma proprio questo il segreto: la satira.

Figura 3 - Il logo della LulzSec_ITA

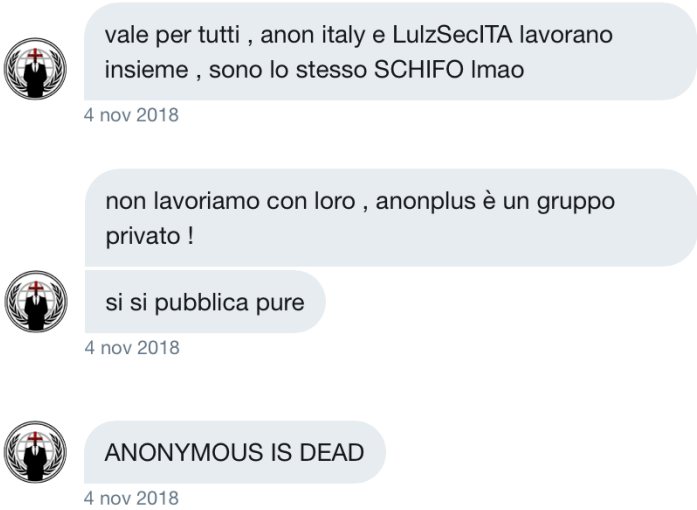
Figura 4 - Il logo di Anonymous Italia

Si inizia dal logo ufficiale di Anonymous, reso leggermente diverso con una personalizzazione del tutto unica e riconoscibile, per poi studiare bene il nome LulzSec che altro non è che la storpiatura di LOL Security: ossia deridere la sicurezza. Ma l'ironia della LulzSec è tutt'altro che sciocca o di poco conto: dietro ogni parola, pesata molto bene, vi è l'astuzia di chi sa come divertire la massa, facendo del sarcasmo, ed è proprio questa parola che contraddistingue il gruppo. La dimostrazione più elevata di questo sarcasmo è arrivata alla fine del 2018, quando dopo un attacco ad alcune forze politiche, il gruppo ne da visibilità con questa immagine.

È impossibile, per chi ha analizzato gli attacchi di Anonymous, non riconoscere la firma di LulzSec, anche se non ci fosse scritto sulla parte superiore lo stile farebbe il resto. Questo conferma che la comunicazione dell'intero gruppo Anonymous è divenuta più efficace, forte, dissacrante, sarcastica e la semplice locandina inizia a fare il giro dei social e finisce su testate editoriali e su quotidiani. L'apporto che LulzSec ha dato ad Anonymous è stato strategicamente fondamentale.

Non è stato censito solo il gruppo Anonymous ma anche gruppi differenti tra cui AnonPlus, responsabile dell'attacco alla SIAE avvenuto a novembre 2018. La differenza tra AnonPlus e Anonymous è fondamentale e sostanziale: proprio durante l'attacco, in un'intervista esclusiva, il gruppo AnonPlus ha definito Anonymous come "morto", prendendo fortemente le distanze dal loro operato.

Di seguito sono riportati alcuni messaggi di AnonPlus intercorsi durante la discussione privata avuta con loro, viene omessa la parte del sottoscritto per ragioni di spazio e formattazione.



L'aspetto importante di questi messaggi è, chiaramente, nella presa di posizione lontana e distante da quella di Anonymous, nonché da una tipologia completamente differente di modalità di attacco. Per molti AnonPlus è molto più efficiente del gruppo Anonymous e ciò li renderebbe assolutamente più temibili in quanto a danni provocati. Su questo ultimo aspetto riguardante le tipologie e le modalità di attacco, è raccomandabile fare riferimento all'apposito capitolo.

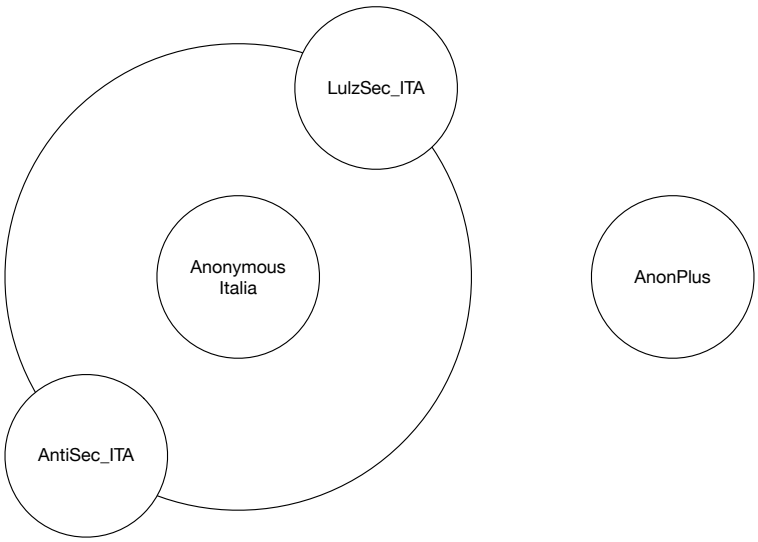


Figura 5 - Mappa degli hacker censiti

Volendo tentare rappresentare graficamente il panorama degli hacker italiani che pubblicamente hanno dichiarato attacchi verso target di vario tipo, potremmo mappare un disegno simile a questo. Da notare come LulzSec e AntiSec possano operare in completa autonomia o portare attacchi sinergici con Anonymous Italia.

Categorie rilevate

Nel tentativo di censire gli attacchi, ci si è resi conto che essi erano molto disparati per tipologia e target: le operations non erano indicizzate da nessuna parte, ogni tanto ne saltava fuori qualcuna e quindi era difficile tenerne conto. È nata quindi l'esigenza di creare una tassonomia che, però, doveva avere al contempo la finalità di classificare l'obiettivo degli attacchi ma anche creare opportune distinzioni. Sono state selezionate al momento 14 categorie.

CATEGORIA	2012	2014	2015	2016	2017	2018	TOTALE
AMBIENTE	1	9	1	3	1	16	**31**
AZIENDE PRIVATE						1	**1**
DIFESA		5					**5**
DIRITTI UMANI				1			**1**
GIUSTIZIA			3		1		**4**
ISTRUZIONE						17	**17**
LAVORO					1	13	**14**
MEDIA				1		13	**14**
POLITICA		4	17	10	2	28	**61**
POLIZIA		4	8	4	1	3	**20**
PROPAGANDA				1		1	**2**
SANITÀ			4			20	**24**
TRASPORTI						1	**1**
VATICANO	33						**33**

La tassonomia è molto complicata da mantenere vi sono ancora dei punti di attenzione che vanno risolti e che è il caso di affrontare quanto prima. Uno tra questi è la differenza tra "*aziende private*" e *"media*": essenzialmente ci sono aziende private che non appartengono all'ambito della comunicazione ma che hanno ricevuto attacchi particolari (ad esempio il caso Iris Ceramiche). Sono state quindi censite ma non sono state inserite in una categoria specifica. Ci sono poi dei messaggi che non sono annoverabili ad un vero e proprio attacco, si tratta di propaganda per far conoscere il gruppo come la opPaperStorm che, in un certo senso, non può essere non censita. Una categoria a parte interessa il Vaticano, con azioni avvenute su parrocchie e associazioni a scopo religioso. È fin troppo chiaro che gli attacchi più frequenti hanno colpito: Politica, Ambiente e Sanità che, non a caso, sono temi estremamente in crisi nel nostro Paese.

Politica

La politica è da sempre uno dei bersagli degli attacchi da parte degli hacker, a dispetto di quanto dichiarato da alcuni esponenti dell'ambiente, non si ritiene che vi sia un partito preferenziale. Anonymous, in particolare, non ha mai manifestato nessuna forma di parzialità nei confronti dei partiti politici, come dimostrato tra l'altro dall'immagine riportata in precedenza. La politica per Anonymous è uno dei centri di maggior problematicità e quindi uno dei bersagli più frequente: viene intesa come la causa di molte ingiustizie che colpiscono il popolo.

Ambiente

L'Italia negli ultimi anni ha subito (e continua a subire) svariate crisi ambientali: la faccenda dell'ILVA, la terra dei fuochi per la Campania, la Xilella e la perdita degli ulivi in Puglia. Sono tutte tematiche che hanno scosso la popolazione, mandando in crisi intere famiglie.

L'emergenza. Xylella, ulivi tutti da abbattere. «La Puglia è in ginocchio»

Nicola Lavacca martedì 22 gennaio 2019

Un emendamento al dl semplificazioni chiede la distruzione obbligatoria delle piante. Ma nella Regione cresce anche il fenomeno dei furti nei campi. Coldiretti: danni per 300 milioni

Anonymous ha assegnato per le crisi più serie delle *operations* e le ha rese attive con attacchi ciclici e molto puntuali, dimostrando la volontà di non voler dimenticare le tematiche oggetto di attenzione e, al contempo, di essere ben presente sul territorio.

Sanità

L'attacco alla sanità pubblica è molto frequente, complice anche una pessima regolamentazione della gestione di portali web, dati sanitari e quanto altro. Nel 2018 alcune ASL sono state oggetto di data breach e andando ad esaminare le tabelle estratte dagli hacker, ci si può facilmente accorgere di come i database MySQL contenessero tipologie di

dati eterogenei e poco adatti a star insieme. Dalle news pubblicate nel portale ai dati dei servizi per i tossicodipendenti. La sanità è senza dubbio uno degli ambiti da consolidare nell'immediato futuro.

Attacchi: tipologie e modalità

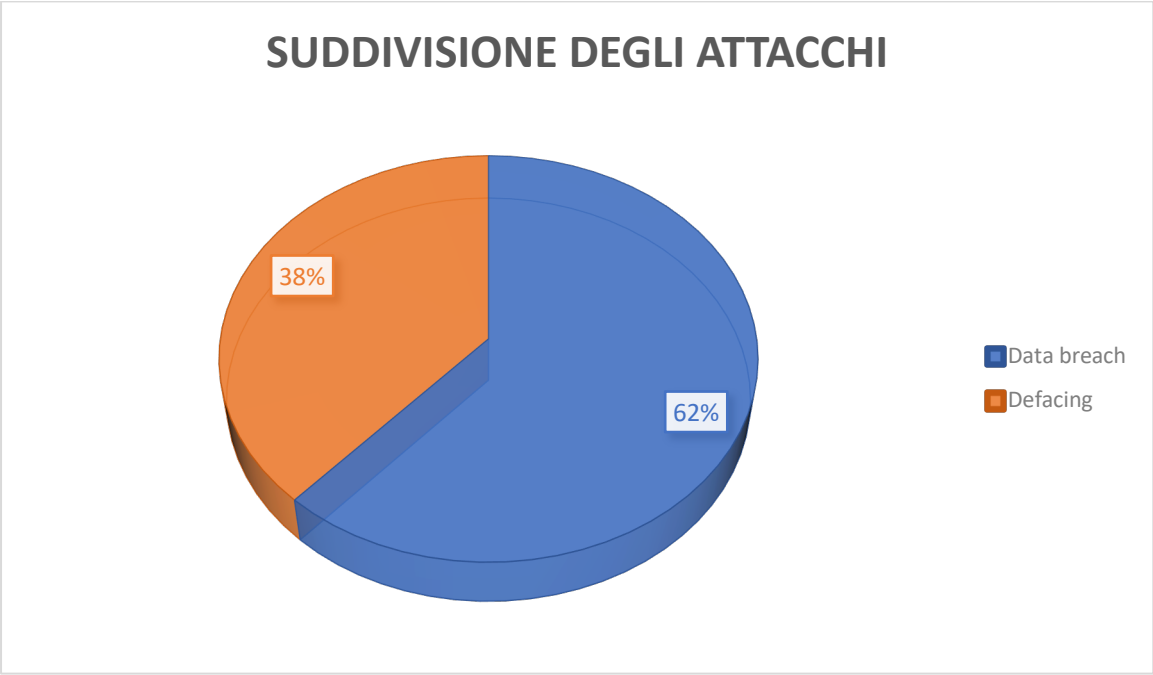
Il 2018 è stato l'anno del data breach: questo termine è rimbalzato su tutti i mezzi di comunicazione di massa grazie anche all'introduzione del GDPR. Il data breach è l'intrusione da parte di personale non autorizzato all'interno di un sistema informatico. Indipendentemente se al suo interno vi siano dati personali o meno, questa azione viene definita data breach (ossia breccia nei dati) ed è disciplinata dal codice penale con l'articolo 615-ter "Accesso abusivo a sistema informatico". L'avvento del GDPR ha reso più "evidente" il danno qualora l'accesso avvenga a dati di natura personale e ha regolamentato le misure da applicare in caso di data breach sia in relazione alle procedure da attuare ex-ante un attacco, sia da attuare quelle ex-post.

Figura 6 - Un esempio di defacing ai danni dell'Accademia Italiana Privacy

Una seconda categoria di attacco è il defacing (defacciamento): si tratta di alterare l'aspetto grafico del sito attaccato principalmente per due scopi:

- Propaganda: generalmente attraverso uno stravolgimento dell'aspetto grafico e l'inserimento dei loghi del gruppo che ha lanciato l'attacco, nonché un messaggio che lo rivendica.
- Lucro: generalmente senza dare visibilità dell'alterazione, allo scopo di far credere ai navigati di essere sul sito originale e in realtà direzionare il traffico verso un sito pirata.

Il censimento è stato condotto suddividendo i casi di data breach da quelli di defacing.



L'attività ha mostrato una maggioranza di attacchi data breach e una leggera minoranza di attività di defacing. Sono stati anche presenti attacchi che hanno avuto solo un'azione di defacciamento. La caratteristica più interessante degli attacchi che hanno contrassegnato il periodo storico osservato è legata alla reazione del "pubblico esperto", indignato molto spesso dall'impiego di strumenti come SQL Map[1].

Si tratta di strumenti gratuiti che permettono di lanciare attacchi a banche dati e siti con lo scopo di saggiarne la resistenza e la sicurezza. Questi strumenti in gergo vengono chiamati strumenti di PenTest (Penetration Test) e sono usati (o dovrebbero esserlo) da sviluppatori ed esperti di sicurezza per testare la resistenza di quanto sviluppato e pubblicato.

L'indignazione nasce dal fatto che secondo molti commentatori questi strumenti sarebbero troppo "banali" per dare dignità ad un attacco e più volte il gruppo Anonymous si è trovato a dover ribattere quanto invece fosse rilevante l'impiego di questi strumenti nella valutazione dello stato del sito: più è banale lo strumento che attacca e "buca" il sito e minore è la sicurezza.

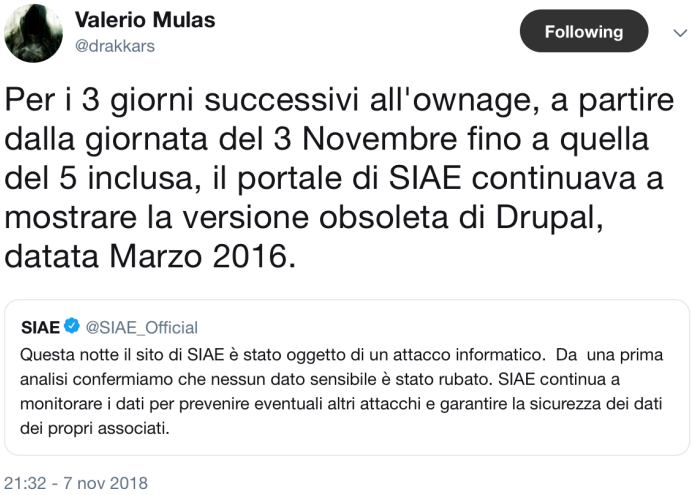
[1] Per approfondire si consiglia: https://www.edoardolimone.com/blog/2018/09/12/sqlmap-tecnica-di-verifica-vulnerabilita-su-db/

In merito alle cause dei breach

È impressionante constatare che praticamente la totalità dei breach ha portato alla luce uno stato di abbandono manutentivo dei portali web colpiti. Carenza o totale assenza di aggiornamenti funzionali sono la principale causa di data breach, anche quando tali aggiornamenti sono rilasciati completamente gratuiti da parte delle software house. Il caso SIAE ha mostrato la mancanza di aggiornamenti al portale Drupal per svariate versioni rilasciate in diversi anni. In un post del 4 novembre 2018, l'amico Dario Buonocore aveva intervistato Dark: del gruppo AnonPlus, ottenendo la risposta[2] che riporto di seguito.

```
<dariobuon> E' stato difficile sfruttare la vulnerabilità ?
<dark> allora usano drupal nn patchato (usavano)
```

Per comprendere quanto fosse grave la situazione del portale SIAE (che è molto simile, se non meno peggio, ad altre realtà hackerate), rimando ad un tweet[3] di Valerio Mulas con cui il 4 novembre abbiamo avuto modo di confrontarci su Twitter.



La carenza di aggiornamenti deve però essere sommata ad una irresponsabile gestione delle password lasciate nei database "in chiaro". Quando un portale web salva la password di un utente può farlo in due modi:

- In modo cifrato, nascondendo la password all'interno di una stringa alfanumerica ad elevata complessità.

[2] Per approfondimenti: https://buonocoresecurity.com/2018/11/04/siae-youve-been-hacked/
[3] Per approfondimenti: https://twitter.com/drakkars/status/1060268754205057026

- In chiaro, rendendola visibile agli hacker che, accedendo al database, possono così leggerla.

La carenza di queste misure di sicurezza va sommata all'adozione di password semplicemente banali anche per gli utenti con ruoli di amministrazione. Non è un caso che nel recente data breach delle PEC dell'Ordine degli Avvocati di Roma, la password dell'utente amministratore fosse di una semplicità disarmante.

Hacking Istituzionale: testare la debolezza dello Stato

In linea generale ciò che preoccupa è che gran parte degli attacchi avvenuti nel 2018 sono stati diretti verso ministeri o verso aziende private che erogano servizi per il pubblico. L'attacco più o meno diretto ad organi di Stato ha l'effetto di indebolire l'immagine percepita della sicurezza informatica del Paese. Sono 17 gli attacchi che, nel 2018, possono essere direttamente collegati all'attività ministeriale del Paese tra cui Ministero dell'Ambiente, della Salute, del Tesoro, dello Sviluppo Economico.

L'immagine collettiva che se ne riceve è piuttosto destabilizzante e sembra lasciar intendere che "nessuno è al sicuro da un data breach", neanche lo Stato.

Principali aspetti di criticità

Adozione delle password

È opportuno ricordare che normalmente gli hacker sono soliti, per ciascuna password in chiaro trovata, crearne versioni cifrate con i più comuni algoritmi per poi avere maggiore facilità nella fase di decodifica. Questo dovrebbe suggerire maggiore cautela nella selezione delle proprie password ed i gestori dei siti dovrebbero prendere accorgimenti che sono noti agli esperti, vale a dire:

- Password lunga più di 8 caratteri
- Usare caratteri alfa numerico simbolici
- Utilizzare maiuscole e minuscole
- Non utilizzare parole di senso compiuto e date
- Cambiare la password almeno una volta ogni 90 giorni

Proprio perché questa attività diventa uno stress per l'utente finale, al quale interessa accedere ai servizi nel modo più semplice possibile, ci si sarebbe aspettati l'adozione di meccanismi di sicurezza adeguati.

Invece è stata disarmante la mancata adozione di misure come, ad esempio, l'autenticazione a due fattori, praticamente quasi mai nemmeno presa in considerazione dai target, a vantaggio di una semplicità e una banalità delle misure di accesso che si sono successivamente mostrate letali per la sicurezza dei dati utenti.

Tempi di reazione molto lenti e non sempre adeguati

A fronte di questi attacchi, tutti rivendicati dai vari gruppi hacker, ci sono stati casi in cui i target hanno avuto forti difficoltà a tornare online con i servizi. Abbiamo citato il caso SIAE che ha fornito una risposta all'accaduto con forti discrepanze rispetto quanto pubblicato dagli hacker e con tempistiche assolutamente inadeguate rispetto alla rapidità di un data breach.

Alcuni siti di partiti politici, è il caso di Fratelli D'Italia, hanno subito bruschi e continui defacing al punto da rallentare le operazioni di ripristino. LulzSec, nel caso di Fratelli D'Italia scatenò l'ilarità di internet con una sequenza di screenshots fin troppo chiara[4].

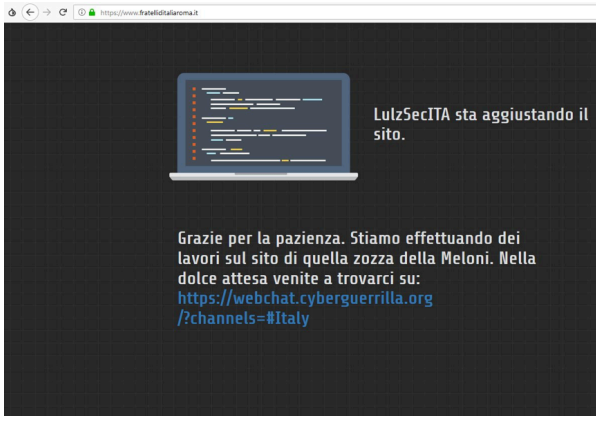


Figura 7 - Defacing del 27/11/2019

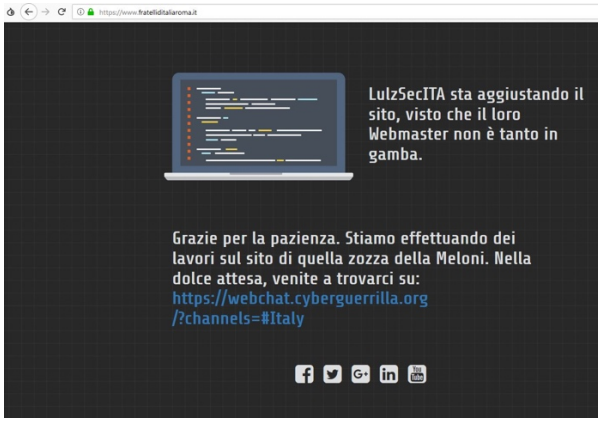


Figura 8 - Defacing del 28/11/2019

Carenza di comunicazione e di organizzazione

Un altro elemento di assoluta criticità è la carenza di comunicazione che, fin troppo spesso, si può presentare in due modi:

- Viene completamente omessa la notizia del data breach da parte del target.
- Vengono omessi alcuni dettagli circa il data breach, tipicamente quelli più delicati e che potrebbero causare un danno reputazione al target.

Comportamenti di questo tipo, ora quantomeno limitati dall'art. 33 del GDPR, sono la dimostrazione della scarsa preparazione delle strutture tecniche ad affrontare fenomeni come data breach e defacing.

Proprio perché l'infallibilità non è un obiettivo raggiungibile in informatica, ci si dovrebbe preparare a dover affrontare situazioni di crisi che possano andare dalla semplice indisponibilità del servizio per ragioni varie, fino all'attacco informatico.

Nel 2018 vi sono stati numerosi casi di completa omissione degli attacchi, cosa che invece non è sfuggita ai naviganti raggiunti direttamente dai tweet lanciati dagli hacker. Il ripristino

[4] Per approfondimenti: https://twitter.com/LulzSec_ITA/status/1067733039470530560

di un servizio a valle di un data breach dovrebbe essere fatto accompagnando le attività tecniche con opportune comunicazioni in merito all'accaduto e alle attività di risoluzione che si intende adottare.

Conclusioni

Non stupisce che il 2018 sia stato definito da molti il peggior anno per la cyber security. Quanto accaduto nel nostro Paese può essere riassunto come una sequenza non gestita di attacchi verso istituzioni, aziende e verso il comparto politico.

Il coraggioso lavoro, svolto dal Garante della Privacy, per promuovere la tutela dei dati personali, deve essere continuato con l'attuazione di quanto previsto dal Regolamento europeo che noi conosciamo con l'acronimo di GDPR.

La mancata attuazione delle sanzioni sarà intesa senza dubbio dagli hacker come l'incapacità a gestire le infrastrutture e proteggere i dati dei cittadini e questo è l'ultimo scenario che deve accadere. Le conseguenze potrebbero essere dannose tanto per il privato, quanto per l'economia dell'azienda.