PUBLIC RELEASE

PHISHING via SMS

Considerazioni sulla modalità di diffusione delle frodi on-line attraverso dispositivi mobili

9 Gennaio 2014

Indice generale

PUBLIC RELEASE

Executive Summary

Il presente documento vuole fornire uno strumento al CIO/IT Manager e agli operatori del settore che permetta di valutare attentamente gli attuali rischi di business legati al campo delle frodi, con particolare riferimento ai crescenti rischi in ambito mobile.

Si tratta di rischi indiretti, collegati a chi commette frodi sfruttando e successivamente danneggiando il nome dell'azienda. E' quindi necessario riflettere sulle metodiche e procedure in uso nelle attività di monitoraggio e contrasto a tale fenomeno, valutando possibili e diverse linee operative di contrasto e gestione di tale specifica tipologia di aggressione informatica.

Il seguente documento presenta un esempio dei rischi potenziali che un'azienda può subire attraverso un'analisi del tentativo di frode recentemente subito a danno dei clienti di un'azienda italiana impegnata nella grande distribuzione, che nel seguito chiameremo per comodità The Company. Questa frode on line della tipologia phishing e' stata perpetrata tramite l'invio di messaggi SMS ed e' stata rilevata da D3Lab nei mesi di Dicembre 2013 e Gennaio 2014,

L'analisi evidenzia la pericolosità di tale tipologia di frode e la difficoltà di svolgere un efficiente monitoraggio, che ha permesso a chi ha commesso la frode di raggiungere un guadagno stimato di oltre 250.000 Euro a fronte di un investimento al di sotto dei 3500 Euro.

Visto il crescente know-how tecnologico dei truffatori e un punto di ingresso economicamente basso, D3Lab stima che il numero di queste truffe possa incrementarsi notevolmente nei prossimi anni.

D3Lab ha l'esperienza e gli strumenti per aiutare la propria clientela nel strutturarsi metodologicamente e operativamente per contrastare questi nuovi fenomeni.

Disclaimer

Sebbene D3Lab abbia proattivamente e tempestivamente avvisato l'azienda colpita dai tentativi di frode dell'accaduto, D3Lab non ha alcun rapporto con essa.

Il presente documento non ha lo scopo di porre in essere valutazioni e giudizi sulle scelte operative dei soggetti colpiti nelle attività di contrasto al fenomeno. La campagna di attacchi a tale società e le risultanze di quanto rilevato da D3Lab vengono descritte e trattate unicamente in forza dell'assoluta atipicità della modalità di attacco via SMS, da noi rilevata per la prima volta a fronte dei rilievi messi in atto sin dal 2009.

Approccio metodologico

L'analisi è stata svolta da D3Lab in base ai rilievi svolti in autonomia attraverso proprie metodiche di monitoraggio del fenomeno phishing, l'esame di messaggi di posta elettronica e di data base di segnalazione on-line, nonché attivando un canale di comunicazione con gli utenti della comunità Internet con la pubblicazione di articoli sul blog D3Lab inerenti le frodi nel seguito trattate, a cui gli utenti hanno potuto apporre commenti realizzando un interscambio di informazioni preziose.

Il presente documento evidenzia la difficoltà di monitorare attraverso i normali canali diffusione, sviluppo e progredire di tali tipologie di frodi, suggerendo un differente approccio informativo a favore del pubblico da parte delle società target, da non identificarsi quale ammissione di una debolezza nella gestione della sicurezza dei clienti, quanto piuttosto da proporre al pubblico quale condotta consapevole delle problematiche di sicurezza derivanti dalle frodi on-line, ricercandone l'utile collaborazione attraverso la costruzione di un virtuoso interscambio di informazioni atto unicamente a tutelare tutte le parti: clienti e società.

Parte delle considerazioni sono basate su ipotesi non essendo disponibile alcuna documentazione ufficiale e pubblica relativa al numero di vittime di tali azioni criminose, all'ammontare del danno economico causato alle vittime, all'effettivo utilizzo degli account di telefonia mobile di cui i criminali hanno fatto uso. Tali informazioni possono essere disponibili, in parte, unicamente a forze dell'ordine, enti emittenti carte di credito e gestori di telefonia mobile coinvolti.

PUBLIC RELEASE

Antefatto

Dal 2012 e per tutto il 2013 si è assistito ad un crescendo di tentativo di frode a danno di società eroganti servizi non bancari, quali rivendita di carburanti, telefonia mobile e fissa, gioco on line, energia e riscaldamento a privati ed aziende, pedaggi autostradali, ecc... con il fine ultimo dei criminali di impossessarsi dei dati delle carte di credito degli utenti.
I criminali attraverso l'invio di messaggi di posta in cui propongono vantaggiose offerte di acquisto, bonus, carte prepagate a costi inferiori al loro valore nominale, facendo talvolta riferimento ad iniziative a favore delle famiglie poste in atto da organi governativi, veicolano i destinatari dei messaggi verso pagine web fraudolente attraverso le quali carpiscono dati anagrafici, codi di carte di credito con relativi codici di sicurezza e credenziali di posta elettronica.

I tentativi di phishing a danno di The Company furono rilevati durante i mesi di Luglio ed Agosto 2012. L'esame dei casi rilevati porto all'individuazione di particolari della struttura dei siti web e dei messaggi di posta fraudolenti chiaramente riconducibili all'operato di entità criminali che tra fine 2012 ed il primo semestre 2013 avevano operato con false offerte di carburante.

In tutti questi casi le società i cui clienti sono scelti quali target dai criminali non ricevono un danno economico diretto, essendo il cliente a venir colpito attraverso l'illecito uso della sua carta di credito.
Tuttavia la società può ricevere un danno di immagine dovuto:

- all'incapacità dell'utente di riconoscere la frode, portato quindi a ritenere che, ingiustamente, non gli venga corrisposto quanto dovuto, ricarica telefonica, carta prepagata per la spesa o bonus carburante che sia;
- alla percezione del cliente di non essere sufficientemente tutelato nell'uso delle risorse e strutture on-line attraverso le quali la società vende o promuove i propri servizi e che i dati personali forniti alla società non siano adeguatamente protetti, come emerge dal commento postato sul blog D3Lab e riportato nell'Illustrazione 6 a pagina 8. Occorre ricordare, a tal proposito, che molti utenti non hanno ancora compreso che le pagine di phishing sono pagine false, fraudolente, slegate dai siti e domini legittimi della società fornitrice di servizi;
- alla reazione di sfiducia nell'approccio comunicativo (SMS o email) utilizzato dall'azienda per proporre offerte e campagne commerciali, che potrebbe generarsi nel pubblico a fronte del protrarsi nel tempo dei tentativi di phishing portati dai criminali con l'uso del medesimo vettore, portandolo ad ignorare le proposte ed offerte della società, se non proprio a cestinare le comunicazioni.

Analisi delle statistiche

L'esame delle statistiche relativa al blog D3Lab evidenziò nella seconda settimana del dicembre 2013 un improvvisa impennata di visite relativamente agli articoli inerenti i tentativi di phishing a danno di The Company e dei suoi clienti. Tale comportamento è spesso stato riscontrato in occasione di campagne di phishing o di diffusione di malware, quando gli utenti meno ingenui cercano notizie di quanto proposto dai messaggi di posta fraudolenti approdando agli articoli da noi redatti a riguardo di similari frodi già avvenute.

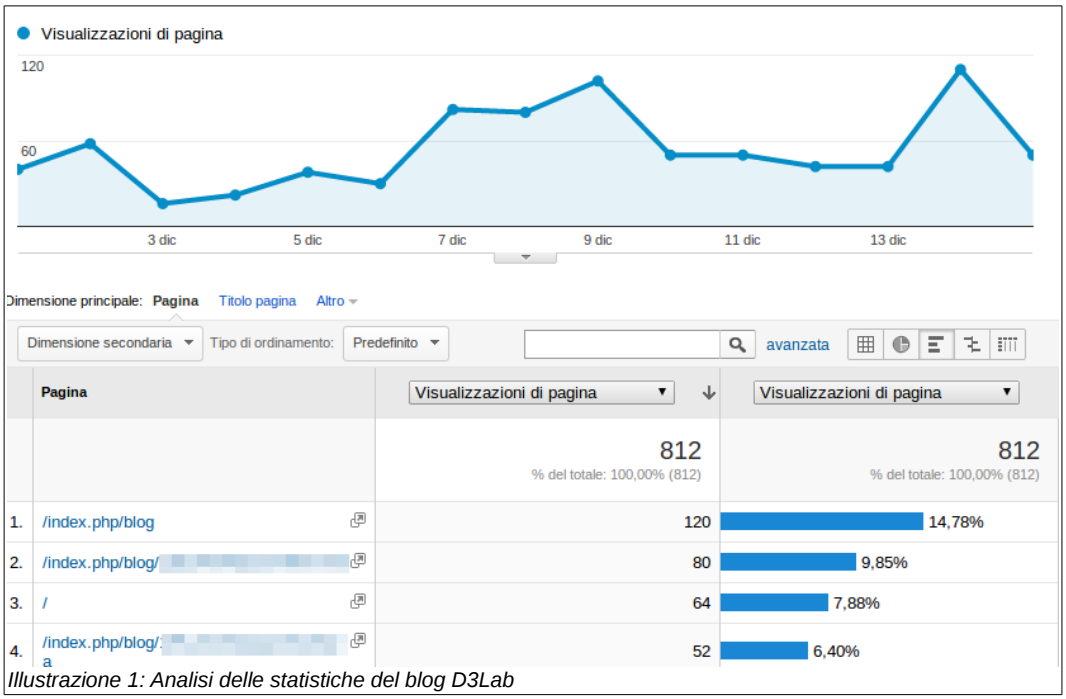

Illustrazione 1: Analisi delle statistiche del blog D3Lab

Tuttavia, per quanto l'analisi delle statistiche e l'esperienza portassero ad ipotizzare nuovi frodi a danno della grande distribuzione, D3Lab non riusciva a rilevare in rete informazioni, evidenze, messaggi di posta o pagine fraudolente riconducibili a ciò.

La segnalazione

Le corrette informazioni pervennero infine attraverso il commento di un lettore del blog che indicò di aver ricevuto il messaggio vettore di attacco via SMS, indicando testo, sito web indicato e numero di telefono mittente.

Successivi rilievi permisero a D3Lab di individuare ulteriori segnalazioni, identificando diversi numeri di telefono da cui i messaggi venivano inviati ed i diversi domini fraudolenti registrati dai criminali.

Breve analisi

Semplificando al massimo la struttura degli attacchi si rileva il posizionamento delle pagine clone nello spazio di domini registrati presso provider italiani, in alcune casi contenenti le pagine clone nel proprio spazio di hosting ed in una minoranza di casi richiamandole da siti web statunitensi attraverso l'uso di frame.

Data segnalazione	Ente	Riferimento	Url attacco
07-01-2014 - 23:34		ref. .2014.3	http://www spa.biz/
05-01-2014 - 23:55		ref. .2014.2	http://www. spa.eu/
01-01-2014 - 17:45		ref. .2014.1	http://www. spa.org/
30-12-2013 - 11:18		ref. .2013.12	http://www.buono .com/
30-12-2013 - 11:17		ref. .2013.11	http://www.super .com/
21-12-2013 - 00:00		ref. .2013.10	http://www. spa.com/
15-12-2013 - 21:55		ref. .2013.9	http://www. buono.org/
14-12-2013 - 10:37		ref. .2013.8	http://www.super com
13-12-2013 - 17:20		ref. .2013.7	http://www. spa.net/

Illustrazione 2: Cloni rilevati

Partendo dal nome del legittimo dominio della società target, thecompany.it, i criminali registrarono diverse possibili varianti, sia facendo uso di altri domini di primo livello, sia realizzando nomi compositi:

- thecompanyspa.net
- thecompanyspa.com
- thecompanyspa.org
- thecompanyspa.eu
- thecompanyspa.biz
- superthecompany.com
- buonothecompany.com
- thecompanybuono.com

L'analisi dei domini attivati dai criminali evidenzia come per quanto una società tenti di tutelare il proprio marchio registrando domini con marchi assimilabili al proprio, non è possibile coprire tutte le varianti rese possibili sia dalla realizzazione di nomi composti (es. thecompany-shop.com) che dall'utilizzo di differenti domini nazionali.

E' doveroso in tal senso ricordare come per l'attacco ai clienti Telepass del 21 Giugno 2012 i criminali abbiano registrato il dominio telepass.lt, con estensione nazionale LT, facente quindi riferimento alla Lituania. Nell'ipotesi che i criminali abbinino al dominio un certificato SSL, nel display di piccole dimensioni di uno smarthphone o di un tablet l'attenzione dell'utente verrebbe attratta principalmente dalla dicitura https in colore verde nella barra degli indirizzi del browser e dal nome dominio di secondo livello, con un'attenzione minimale posta al dominio nazionale “lt” facilmente confondibile con l'italiano “it”.

Il monitoraggio continuo e costante dei tentativi di phishing rimane quindi un imprescindibile sistemi di tutela di marchio, immagine e clienti aziendali.

PUBLIC RELEASE

Informazione e aggiornamento bidirezionali attraverso il blog

L'attuale politica di D3Lab prevede la pubblicazione sul blog aziendale di articoli relativi a frodi e tentativi di phishing rappresentanti una novità perché inerenti ad enti precedentemente non colpiti, realizzati con metodiche nuove o poco conosciute, implementati elementi di novità di rilievo; ciò in contrapposizione alla politica di segnalazione dei singoli attacchi adottata precedentemente al 2012 quando la strutturazione dell'azienda era solo in fase di progetto embrionale.

Proprio in osservanza di tale politica, rappresentando il tentativo di phishing veicolato attraverso SMS una novità nel panorama italiano, successivamente ai rilievi effettuati, D3Lab pubblicò sul proprio blog un primo articolo relativo al fenomeno in cui si descriveva la modalità attuativa della frode rilevata.

In coincidenza con la festività del Primo dell'Anno (2014) le statistiche del blog presentarono una vertiginosa impennata di visite all'articolo sopra citato e D3Lab fu contattata telefonicamente da utenti che, giunti sul blog aziendale attraverso l'utilizzo dei motori di ricerca, chiedevano conferma della veridicità dell'offerta giunta via SMS. Gli utenti del web individuavano l'articolo inerente la frode ricercando sul web parti del testo presentato nell'SMS, il numero di telefono da cui i messaggi provenivano o i nomi dominio utilizzati dai criminali e riportati negli articoli.

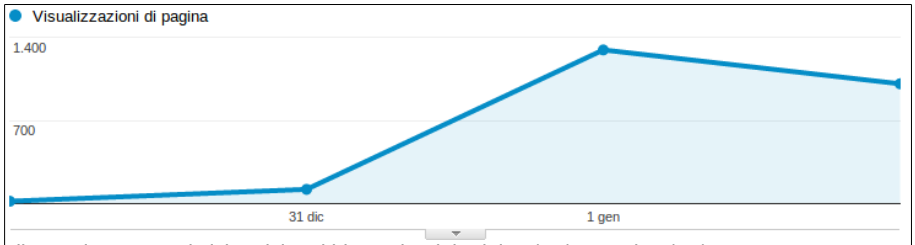

Illustrazione 3: statistiche visite al blog aziendale dal 30/12/2013 al 02/01/2014

In risposta all'evidente dimostrazione di interesse D3Lab pubblicò un secondo articolo finalizzato a fornire un'informazione più completa. In risposta all'iniziativa e nello spirito di autotutela della comunità digitale, gli utenti cominciarono a fornire, attraverso i commenti agli articoli, costanti informazioni relative ai domini indicati negli SMS fraudolenti ed ai numeri di telefono da cui questi provenivano.

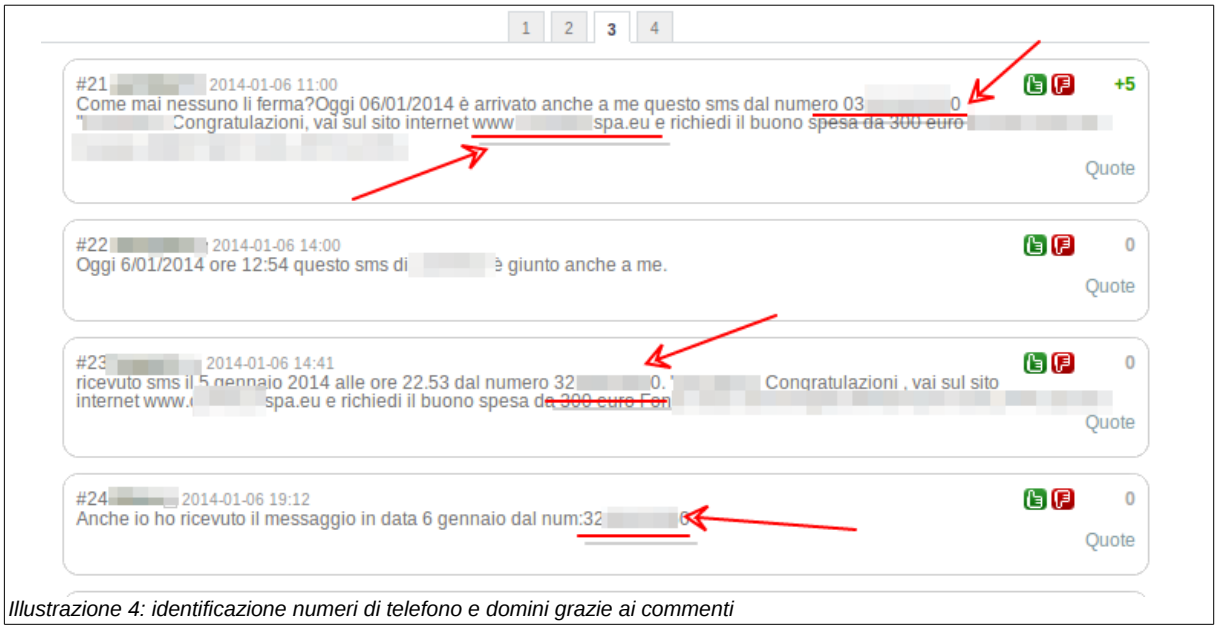

Illustrazione 4: identificazione numeri di telefono e domini grazie ai commenti

I commenti dei visitatori evidenziano inoltre come, in questo momento di crisi economica e ristrettezze per le famiglie, i criminali abbiano individuato il giusto tasto/pretesto su cui far pressione per portare gli utenti a visitare le pagine fraudolente.

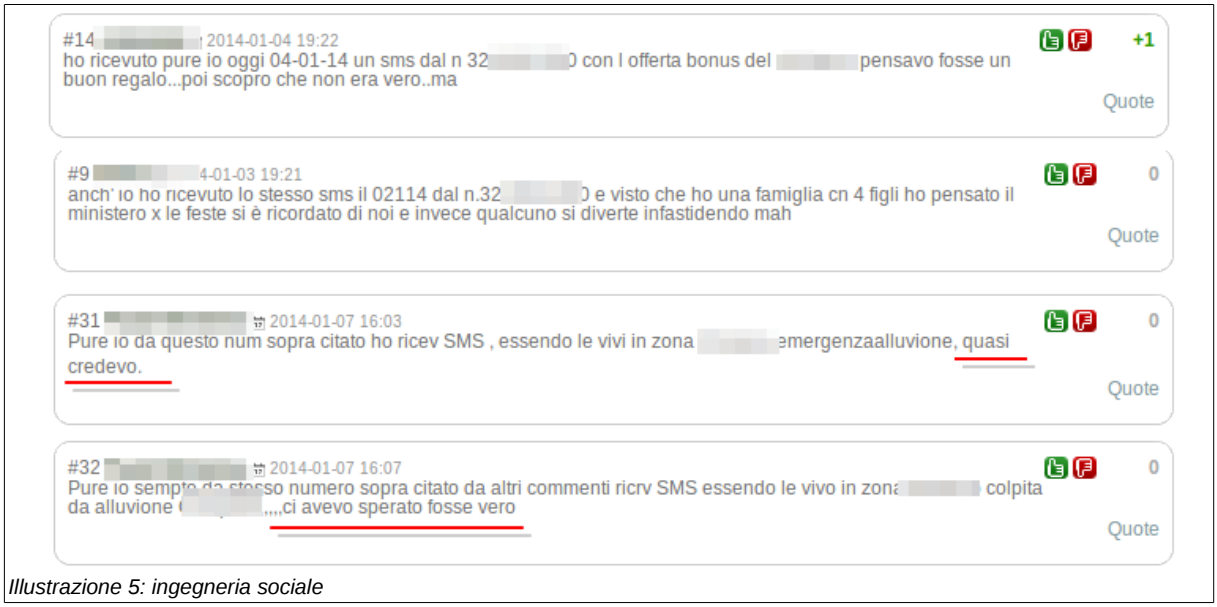

Illustrazione 5: ingegneria sociale

In fine un commento pone l'attenzione su un possibile problema di sicurezza delle informazioni, nello specifico di privacy e dati personali dei clienti, ipotizzando una possibile fuoriuscita di informazioni dai data base della società bersaglio.

Illustrazione 6: dubbio

Utilizzo delle informazioni ricevute dal pubblico

I commenti dei lettori del blog hanno permesso di continuare a tracciare il posizionamento delle pagine web fraudolente in un momento in cui il monitoraggio dei canali tradizionali, causa l'utilizzo dei messaggi SMS, si è rivelato di scarsa efficacia .

Le informazioni fornite dai lettori avrebbero quindi consentito di attivare idonee procedure e richieste finalizzate alla messa off-line delle pagine fraudolente e dei domini coinvolti.

L'indicazione dei numeri di telefono dai quali venivano inviati i messaggi permette, inoltre, di dettagliare denunce/querele presentate dai soggetti titolati, nel caso specifico la società target, presso le forze dell'ordine e la magistratura, consentendo lo svolgimento di accertamenti investigativi finalizzati all'identificazione degli autori delle frodi.

In Internet sono facilmente individuabili servizi di call ed SMS spoofing[1], che consentono cioè la realizzazione di chiamate telefoniche e l'invio di messaggi SMS falsificando il numero dei telefono del chiamante/mittente. Tali servizi richiedono l'acquisto di un credito pagato con carta di credito, operazione che il criminale può facilmente fare attraverso circuiti e strumenti deputati ad anonimizzare la sua navigazione in rete e facendo uso di carte di credito di cui ha precedentemente carpito i dati ad ignare vittime. Tuttavia il costo di tali servizi è maggiore di quello

1 http://www.spoofingcall.com/

per lo svolgimento delle medesime attività con l'uso di schede SIM comuni, che non di rado il criminale riesce a procurarsi con la collaborazioni di soggetti inconsapevoli dell'uso che verrà poi fatto delle schede SIM da loro attivate.

Verifica dell'ipotesi "information dump"

La cronistoria degli incidenti informatici e delle violazioni di sistemi aziendali ci ha abituato, con i casi Sony e Adobe, tanto per citare i più famosi, alla possibilità che informazioni inerenti gli utenti/clienti di una società vengano carpite in modo illegittimo. I casi che hanno raggiunto la ribalta dei media sono tuttavia stati caratterizzati dal rilascio dei *dump,* o *leak* che chiamar li si voglia. Ad ora, dalla rete non è mai giunta notizia di un incidente di tale tipologia a danno di The Company.

Tuttavia l'ipotesi, se verificata, avrebbe configurato uno scenario di elevatissimo rischio. Per comprendere pienamente il problema creiamo uno scenario ipotetico:

> *La società MyClothes Online SpA si occupa di vendita di di abbigliamento di marchi prestigiosi attraverso Internet. I clienti all'atto della registrazione presso il portale web inseriscono dati personali quali il numero di cellulare e l'indirizzo e-mail.*
>
> *Se ipotizziamo una qualche connivenza tra criminali dediti al phishing e dipendenti della MyClothes Online SpA, designata quale target dai criminali, appare evidente come la trasmissione all'esterno di informazioni relative ai clienti, anche ristrette al solo numero di telefono e indirizzo di posta elettronica, ponga i criminali in una posizione di forza, assicurando loro di poter veicolare una falsa comunicazione (offerta commerciale, richiesta di verifica dati, ripristino account, ecc...) verso un pubblico sicuramente legato al target e presumibilmente ricettivo. Se poi il canale attraverso cui veicolare la frode è un canale normalmente utilizzato dalla società target per trasmettere informazioni e campagne commerciali si può dire, riprendendo una nota pubblicità, che ai criminali "piace vincere facile".*

Trasmigriamo quindi l'ipotetico scenario sopra ipotizzato nel caso concreto degli attacchi a danno degli utenti The Company, ipotesi riportata anche dal commento apparso sul blog D3Lab, visibile nell'Illustrazione 6 alla pagina precedente. Appare lecito domandarsi quale danno si sarebbe potuto avere se un insider avesse veicolato all'esterno i numeri di telefono dei titolari di carte di fidelizzazione, già per altro abituati a ricevere comunicazioni commerciali via SMS dalla società.

Non si sta quindi ipotizzando uno scenario di spear phishing nei confronti di dipendenti, realizzato per ottenere una testa di ponte nella rete di una specifica azienda, ma di un phishing tradizionale realizzato su un target di utenti sicuramente legati alla società bersaglio, senza quindi il tipico spreco di spedizioni del veicolo d'attacco (SMS o email) verso utenti che nulla hanno a che fare con il target, come accade nelle frodi a cui siamo stati fino ad ora abituati e che vedono spesso soggetti non clienti delle società ricevere le false mail essendo i loro indirizzi stati raccolti in rete dai phisher o creati con modalità automatica in base ai nomi più comuni.

Per verificare tale ipotesi D3Lab ha contattato i lettori del blog che, commentando gli articoli sopra citati, hanno lasciato un loro recapito di posta elettronica, chiedendo se fossero effettivamente clienti The Company fidelizzati da un qualche tipo di iscrizione, formula, offerta o carta. Le risposte, in realtà poche, sono state tuttavia sufficienti ha fugare il dubbio, essendo subito emerso che alcuni dei destinatari dell'SMS non erano mai stati legati alla società The Company in questione in alcun modo.

Si può quindi asserire che a monte dell'attacco non vi è stata alcuna fuoriuscita di informazioni personali dai sistemi di The Company, che non appaiono coinvolti direttamente, non appare quindi lecito trarre conclusioni sulla sicurezza del sistema stesso.

Occorre sottolineare come un'indagine condotta su tale tipologia di frode consenta di individuare non solo la presenza di "insider" veri e propri, ma anche di anelli deboli nella struttura e nel flusso

di gestione delle informazioni personali e dei dati sensibili in possesso di una società e/o di aziende con essa collaboranti, quali ad esempio fornitori di servizi con i quali l'azienda condivide per le proprie finalità commerciali ed operative tali dati.

Verifica dell'ipotesi "ricerca in rete"

La seconda ipotesi che D3Lab ha voluto verificare è quella che i numeri di cellulare dei destinatari dei messaggi SMS fossero stati raccolti attraverso l'uso automatizzato dei motori di ricerca. Si è quindi richiesto a coloro che avevano commentato gli articoli pubblicati sul blog D3Lab di fornire il numero di telefono sul quale avevano ricevuto l'SMS fraudolento. Le risultanze delle ricerche condotte hanno immediatamente evidenziato che solo una minima parte dei numeri in questione erano individuabili in Internet in quanto pubblicati in annunci di lavoro o di acquisto/vendita di beni on-line.

A fronte delle verifiche effettuate è quindi ipotizzabile che i criminali abbiano realizzate le liste di numeri di telefono verso i quali effettuare l'invio degli SMS attraverso l'uso di strumenti automatici.

Ipotesi di rendimento

Una valutazione di quanto guadagnato dai criminali con gli attacchi di phishing portati in meno di un mese nei confronti dei clienti di The Company può essere solo ipotizzata, non essendo possibile per D3Lab avere accesso a dati numerici concreti.

Si consideri innanzi tutto la spesa sostenuta dai criminali per l'approntamento, nel corso del mese di attacchi, della necessaria struttura: la registrazione di domini presso i provider italiani usati ha un costo di circa 35,00 Euro caduno, l'hosting presso il provider statunitense di circa 6,95 $/mese, il che porta ad una spesa per la "struttura digitale" impiegata da dicembre a meno di 400,00 Euro. Ipotizzando un costo di invio SMS di 0,15 Euro, il massimo attualmente, per l'invio di 20.000 SMS i criminali avrebbero speso 3.000 Euro. Si ha quindi un ammontare di spesa inferiore ai 3.400 Euro.

Per la valutazione del danno portato ricorriamo ad alcune stime ed ipotesi partendo dai dati desunti dalle statistiche del blog D3Lab. I primi sette giorni di Gennaio 2014 hanno contato oltre 11.000 visualizzazione dei due articoli del blog aziendale inerenti la frode a danno di The Company esaminata nel presente documento, con oltre 5.000 visitatori unici. E' ipotizzabile che queste 5.000 visualizzazione uniche siano dovute a ricerche di informazioni relative alla frode svolte in rete da chi ha ricevuto l'SMS fraudolento. Allo stato attuale, tuttavia, non è possibile sapere quale percentuale rappresentino questi visitatori rispetto al totale di coloro che hanno ricevuto l'SMS vettore di attacco dal primo gennaio. Considerando la bassa alfabetizzazione informatica del nostro paese è ipotizzabile che molti di coloro che hanno ricevuto il messaggio non abbiano mai effettuato alcuna ricerca in Internet, né visitato le pagine proposte dai criminali.

	Pagina	Visualizzazioni di pagina uniche	Visualizzazioni di pagina
		5.688 % del totale: 100,00% (5.688)	12.773 % del totale: 100,00% (12.773)
1.	/index.php/blog/	3.457	59,94%
2.	/index.php/blog/1 ...g-	1.681	29,16%
3.	/	103	2,02%
4.	/index.php/blog/152-phishing-	92	1,46%
5.	/index.php/blog	79	1,72%
6.	/index.php/servizi	59	1,21%
7.	/index.php/contatti	51	0,94%
8.	/index.php/formazione-corsi	37	0,80%

Illustrazione 7: statistiche visite blog D3Lab dall'1 al 7 gennaio 2014

Ipotizziamo quindi che in questa prima settimana 2014 i destinatari degli SMS criminali siano stati il doppio dei nostri visitatori unici, circa 10.000. Considerando che la frode è in atto dalla metà dello scorso dicembre, risulta realistico ipotizzare un totale di almeno 20.000 messaggi SMS mandati a destinazione dall'inizio della campagna di phishing.

Se il numero di messaggi SMS ipotizzato appare esagerato è opportuno evidenziare come l'analisi dei siti di phishing abbia più volte permesso il recupero delle liste di indirizzi di posta elettronica usate dai criminali per l'invio dei messaggi fraudolenti, contenenti dai 29.000 agli 467.000 indirizzi email differenti.

In base all'esperienza D3Lab gli ammanchi sulle carte di credito, i cui numeri vengono “acquisiti “ dai criminali attraverso attacchi di phishing, può variare tra i 250 ed ai 2.500 Euro. Per le valutazioni del caso, al fine di ottenere un dato realistico:

- sottostimiamo volutamente i possibili ammanchi causati dai criminali agli utenti, ipotizzando quindi una illecita spesa per un importo di soli 250 Euro;
- consideriamo che solo il 5 % del totale ipotizzato di riceventi l'SMS, quindi 1.000 utenti, sia stato ingannato dal messaggio e dalle false pagine web, cadendo vittima dei criminali;

i criminali avrebbero dunque incassato, in meno di un mese, almeno 250.000 Euro, il 7000% di quanto speso.

Si tratta naturalmente solo di una stima, assolutamente non verificabile. Solo i gestori di telefonia a cui fanno capo i numeri di telefono da cui sono stati inviati gli SMS sono in grado di dire quanti messaggi siano stati effettivamente inviati, informazione acquisibile da forze dell'ordine e magistratura. Queste, tuttavia, difficilmente hanno modo di correlare eventuali denunce/querele agli attacchi di phishing in discussione in quanto, spesso, le vittime del phishing non sono in grado di correlare l'ammanco subito ad uno specifico evento (e-mail ricevuta o visite a specifiche pagine fraudolente). Allo stesso problema soggiaciono istituti bancari ed enti emittenti carte di credito, anch'essi nell'impossibilità di correlare gli ammanchi a danno dei clienti con specifici tentativi di frode.

A chi ritiene il risultato dell'ipotesi precedente eccessivo occorre forse riportare dati di prima mano:

- l'attacco di phishing del 21 Giugno 2012 contro i clienti Telepass portò nelle mani dei criminali 51 codici di carta di credito in una sola giornata;
- in uno dei recenti attacchi volti a colpire i clienti di uno dei gestori di telefonia mobile italiani i criminali conquistarono 21 codici di carta di credito validi in sole 12 ore.

Se si volesse tuttavia essere più cauti si potrebbe ridimensionare le stime, ipotizzando solo 100 vittime, rappresentanti lo 0,5 % dei presunti 20.000 destinatari degli SMS fraudolenti: in tale ipotesi i phisher avrebbero incassato 25.000 Euro, il 735% di quanto speso.

La possibile risposta della società colpita

Astraendoci dal caso concreto degli attacchi alla società, indicata nel presente documento come “The Company”, realmente colpita dagli attacchi rilevati, possiamo ipotizzare in base all'esperienza ed alla conoscenza delle modalità operative quale sarebbe stato l'approccio più probabile, in panorama italiano, per strutturazione di una risposta per questa tipologia di incidente da parte di una ipotetica società di livello nazionale.

Shutdown

La finalità della società scelta quale target dai criminali è quella di rendere inefficace il tentativo di phishing, risultato ottenibile con la messa off-line delle pagine fraudolente riproducenti elementi grafici, template, logo e marchio della società stessa. Tale azione viene usualmente realizzata attraverso:

- chi amministra il sito/server nel quale i criminali hanno inoculato le pagine fraudolente;
- il fornitore di hosting;
- il fornitore di connettività;

i quali, notiziati delle attività illecite messe in atto da criminali facendo indebito uso delle loro strutture ed in violazione dei termini di servizio, intervengono cancellando le pagine web fraudolente o sospendendo i domini creati dai criminali, oppure dagli stessi violati, quando l'azione di “pulizia” da parte del legittimo amministratore non è tempestiva.

Affinché tale azione di “messa off-line” possa attuarsi è necessario conoscere l'indirizzo delle pagine web fraudolente, informazione a cui si giunge attraverso il monitoraggio di mail box, servizi di warning e/o avvalendosi di servizi di monitoraggio quali quello realizzato da D3Lab.

Informazione sul web

Le aziende, in particolare istituti bancari, ma anche fornitori di servizi internet quali posta elettronica, cloud, ecc..., classici obbiettivi cronicizzati delle frodi tipo phishing, al fine di informare gli utenti dell'esistenza della minaccia approntano sui propri siti web pagine informative, usualmente raggiungibili con link riportati in home page, nelle quali illustrano le caratteristiche della minaccia phishing, come riconoscerla ed evitarla.

Società di tipo diverso, che usano il web principalmente come vetrina per i propri prodotti e le proprie offerte, non offrendo direttamente servizi, non richiedendo operazioni di login e non avendo subito precedenti di tentativi di frode portati nei confronti dei loro utenti da parte di criminali attraverso il web, è possibile non abbiano mai svolto verso i clienti un'azione informativa relativa al phishing, e si trovino quindi nell'esigenza di intervenire tempestivamente al presentarsi della minaccia.

Operando nell'analisi del phishing dal 2009 D3Lab ha rilevato come sovente l'utente di Internet medio tenda, durante la fruizione dei servizi erogati attraverso il web dalle diverse società (ricerca e acquisto prodotti, accesso ai servizi di comunicazione, gestione di servizi per la casa, il lavoro e la persona) ad ignorare bellamente i link proposti, anche in home page, verso le pagine informative relative alla sua sicurezza, essendo completamente assorbito dall'espletamento dei propri affari o dalla propria esperienza multimediale.

In tale ottica, in risposta alle contingenti necessità di reazione ad una specifica, aggressiva ed innovativa campagna di phishing, come quella realizzata dai criminali con l'invio di messaggi SMS, potrebbe essere necessario ipotizzare di informare “forzatamente” il cliente dell'esistenza di una temporanea situazione di serio pericolo, rendendo inoltre possibile l'individuazione delle pagine informative e di notizie relative alla contingente minaccia attraverso i motori di ricerca che, come mostrato dall'analisi del statistiche del nostro blog, rappresenta uno strumento sempre più utilizzato dagli internauti per cercare conferme e/o notizie in relazione a offerte, servizi, campagne di marketing proposte dalle aziende di cui sono, o potrebbero, essere clienti.

Informazione reciproca azienda-pubblico-azienda

E' opportuno sottolineare nuovamente come l'uso dei messaggi SMS quali veicoli dell'attacco, abbia leso l'efficacia dei monitoraggi tradizionali, rendendo limitata l'utilità dei tradizionali canali quali mail box e servizi di segnalazione.

In tale ottica il maggior supporto alle società target nella fase di monitoraggio e quindi di identificazione di nuovi siti clone, può venire unicamente dai clienti, dagli internauti, scelti dai criminali quali destinatari dell'SMS di attacco.

La capacità della società target di liberarsi dall'erronea convinzione che minimizzando incidenti e minacce sia possibile tutelare la propria immagine aziendale, fornendo in caso di “crisi phishing” una corretta e puntuale informazione all'utente del web, le consentirà di acquisire, proprio dagli utenti, allestendo ad esempio apposite pagine di segnalazione o la possibilità di apporre commenti alle pagine informative, importanti e preziose informazioni atte a permettere di tracciare l'evolversi dei tentativi di frode in atto e di inoltrare le necessarie richieste di messa off-line delle pagine fraudolente individuate.

I numerosi commenti postati dai lettori agli articoli pubblicati sul blog D3Lab confermano la fattibilità e utilità di questo interscambio di informazioni.

Informazione sui social network

Sul fronte social network la società target potrebbe trarre vantaggio, sia in termini operativi che di immagine, dall'uso dei social netowork che raccolgono maggiori consensi tra il pubblico, Facebook e Twitter, su cui molte società hanno già da tempo allestito proprie pagine e profili.

Opinione di D3Lab è che sottacere l'esistenza di una momentanea crisi, quale può essere un contingente attacco di phishing, potrebbe avere più risvolti negativi che positivi dal momento che comunque gli attacchi verrebbero rilevati dagli utenti del web che, in risposta alla spirito di condivisione delle informazioni ed autotutela della comunità web ne darebbero notizia, generando nel pubblico l'idea di una condotta reticente da parte dell'azienda.

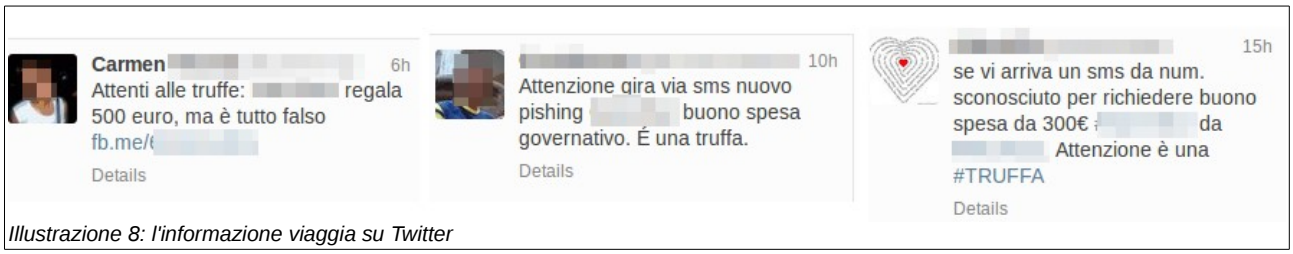

Illustrazione 8: l'informazione viaggia su Twitter

Usare quindi i social network informando il pubblico dell'esistenza di una momentanea situazione di aggressione nei confronti dei clienti della società, come fatto su Facebook[2] da H3G Italia in data

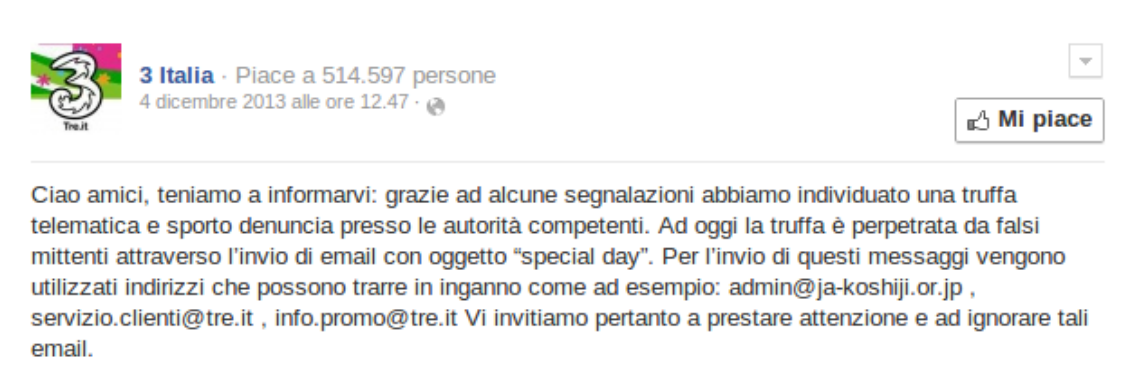

Illustrazione 9: Warning di H3G Italia a tutela degli utenti

4 Dicembre 2013, potrebbe portare apprezzamento da parte degli utenti, generando in essi un

2 https://www.facebook.com/3Italia/posts/10153541617730099

sentimento di fiducia nei confronti dell'azienda per l'attenzione riposta alla loro sicurezza, come sembrano dimostrare l'oltre mezzo milione di “mi piace” raccolti dal post riportato nell'Illustrazione 9, nonché innescare quello scambio di informazioni reciproco azienda-pubblico-azienda tanto utile all'azione di monitoraggio ed al successivo contrasto della frode.

Conclusioni

L'analisi degli attacchi di phishing portati a mezzo SMS evidenzia:

- la pericolosità di tale tipologia di frode, la dove i criminali possano contare su recapiti telefonici sicuramente appartenenti a clienti dei servizi erogati dalla società target;
- la difficoltà di svolgere un efficiente monitoraggio, ineludibile premessa per un efficace contrasto, la dove il mezzo scelto quale vettore della frode, l'SMS, non consente di individuare frodi in atto e pagine fraudolente attraverso l'analisi di mail box e data base di segnalazione dei casi di phishing.

L'attività informativa svolta da D3Lab attraverso gli articoli inerenti tali frodi pubblicati sul blog aziendale, ha evidenziato la possibilità di un utile scambio reciproco di informazioni con gli utenti che permette la tempestiva individuazione delle pagine web fraudolente e la certa identificazione dei numeri di telefono da cui gli SMS vengono inviati.

Appare quindi opportuna valutare preventivamente come agire in caso la propria società ed i clienti della stessa divengano il target di criminali operanti con le modalità sopra descritte, considerando:

- se un “basso profilo” sul web e sui social network a tutela dell'immagine aziendale possa rappresentare un effettivo vantaggio, o possa trasformarsi in un boomerang nel caso la comunità web interpreti il “basso profilo informativo” quale condotta reticente;
- l'utilizzo dei social network e degli strumenti da questi messi a disposizione, nello specifico gli hashtag[3], quale utile ausilio all'azione di monitoraggio dei tentativi di frode, sebbene imprescindibile dalla collaborazione del pubblico di utenti e da una necessaria pubblica ammissione dell'esistenza della specifica minaccia in un dato istante temporale;
- l'esigenza di formare adeguatamente il personale dei call center affinché l'operatore non si limiti a dare conferma al cliente chiamante della frode in atto, ma possa operare quale valido ausilio all'azione di monitoraggio richiedendo informazioni essenziali quali url e numeri di telefono da cui il messaggio criminale è partito.

Si ringraziano :

Edgardo V., Claudio T., Giuseppe P., Andrea D., Mario P., Gianni A., Dario P., Raul C.

3 http://it.wikipedia.org/wiki/Hashtag