UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI INFORMATICA

Corso di Laurea in Sicurezza dei Sistemi e delle Reti Informatiche

Phishing: tecniche e strategie di un fenomeno in evoluzione

RELATORE

Prof. Nello SCARABOTTOLO

TESI DI LAUREA DI

Andrea DRAGHETTI

Matr. 778883

Anno Accademico 2018/2019

Indice

1. Introduzione

Il phishing è un tentativo fraudolento di ottenere informazioni sensibili ingannando la vittima attraverso la ricezione di una comunicazione apparentemente affidabile. Generalmente in un attacco di phishing su larga scala vengono carpiti nomi utenti, indirizzi email, password e dettagli delle carte di credito; invece, per attacchi di phishing mirati ad utenti o ad aziende il tentativo fraudolento potrebbe carpire altre informazioni riservate.

L'ingegneria sociale è la principale tecnica utilizzata per ingannare l'utente in un tentativo di phishing; un ingegnere sociale (social engineer) deve sapere fingere ed ingannare la vittima dell'attacco al fine di carpire informazioni utili.

Il termine phishing è una variante di Fishing (pesca); la sostituzione ortografica di "f" con "ph" è probabilmente influenzata dal termine Phreaking[1]. Quest'ultimo è un termine sfruttato negli anni '60 per indicare chi studiava ed analizzava i sistemi telefonici.

Il phishing viene effettuato da una persona o da un team di persone definite Phisher(s), coloro che tentano di ingannare l'utente e di carpirgli informazioni riservate.

[1] http://itre.cis.upenn.edu/~myl/languagelog/archives/001477.html

2. Storia

Una prima tecnica tecnica di phishing è stata descritta in un documento e in una presentazione all'International HP Users Group, Interex nel 1987[2].

Il termine phishing è stato per la prima volta menzionato nel software di hacking AOHell[3] nel 1995; il software includeva un tool per creare campagne di phishing atte a carpire password e dati delle carte di credito ai danni degli utenti del portale America Online (AOL). Il tool impediva l'accesso al sito ufficiale di AOL generando messaggi istantanei come: "Hi, this is AOL Customer Service. We're running a security check and need to verify your account. Please enter your username and password to continue.". Negli stessi anni il termine phishing veniva citato nella popolare newsletter "2600"[4].

Gli anni 2000 hanno portato ad una vera e propria escalation di attività fraudolente veicolate tramite il phishing; a Giugno del 2001 si è registrata la prima attività ai danni di un circuito di pagamento, e successivamente si è verificata una campagna mirata a seguito degli attentati dell'11 Settembre 2001 in cui veniva inviata una richiesta fraudolenta di verifica dell'identità degli utenti.

Nel 2005 il Regno Unito ha subito quasi un raddoppio[5] delle perdite dovute a frodi nel web banking, principalmente dovute al phishing, da 12 milioni di sterline nel 2004 a oltre 23 milioni nel 2005. Nel medesimo anno la AOL UK[6] ha condotto una ricerca sugli utenti inglesi e su un campione di 2mila utenti del web ha constatato che il 5% di questi aveva già subito un danno patrimoniale a causa del phishing.

Il 2006 grazie al crescete utilizzo dei Social Network[7], in particolare della piattaforma MySpace, vede le prime attività di phishing ai danni degli utenti delle piattaforme sociali. Le informazioni personali divulgate dagli utenti nei social network possono essere utilizzate per compiere un furto di identità.

---

[2] Interex Proceedings, vol. 8, September 1987, p. 6.

[3] https://en.wikipedia.org/wiki/AOHell

[4] http://www.technicalinfo.net/papers/Phishing.html

[5] https://www.finextra.com/news/fullstory.aspx?newsitemid=15013

[6] https://www.theregister.co.uk/2005/05/03/aol_phishing/

[7] https://web.archive.org/web/20060616110238/http://www.pcworld.com/resource/article/0%2Caid%2C125956%2Cpg%2C1%2CRSS%2CRSS%2C00.asp

Il Gartner[8], una società di consulenza e ricerca internazionale, ha condotto un sondaggio nel 2007 dichiarando che 3,6 milioni di persone da Agosto 2006 ad Agosto 2007 hanno perso a causa del phishing 3,2 miliardi di dollari. L'importo medio sottratto ad ogni vittima è di 886 dollari, contro i 1244 dollari dell'anno precedente; le vittime del 2007 hanno inoltre recuperato il 64% delle loro perdite mediante rimborsi o annullamenti di transazioni, contro il 54% recuperato nel 2006.

Nel 2007 PayPal ed eBay sono i marchi che subiscono maggiormente le attività di phishing; e le comunicazioni sono sempre più sofisticate grazie ad un uso più attento dell'ingegneria sociale. L'intento dei criminali è principalmente quello di rubare dati delle carte di credito o credenziali dei conti correnti, e vengono colpite aree geografiche in cui il contrasto e il rilevamento del phishing è più debole.

Nel 2007 in Italia vi fu la prima sentenza[9] per attività di phishing da parte del Tribunale di Milano, sentenza confermata poi in Cassazione nel 2011. I phisher[10] effettuavano principalmente attività ai danni dell'istituto Poste italiane S.p.A.; una volta sottratte le credenziali di accesso degli utenti provvedevano a trasferire il denaro su carte PostePay intestate all'organizzazione criminale, e successivamente sfruttavano gli sportelli automatici delle case da gioco per prelevare le somme sottratte, poiché avevano limiti di prelievo giornaliero molto più alti rispetto ai tradizionali ATM.

La TD Ameritrade[11], una delle principali società Americane di broking per le attività finanziarie, nel 2007 ha subito un'importante violazione del database centrale acconsentendo ai criminali di rubare oltre 6 milioni di indirizzi email. Sebbene gli attaccanti non riuscirono direttamente ad estrapolare ulteriori informazioni presenti nel database, avviarono una massiccia campagna di phishing verso i 6 milioni di utenti per ottenere anche nomi utenti e le password.

A gennaio 2009 la Experi-Metal Inc.[12] ha subito un attacco di spear phishing, probabilmente il più importante fino ad allora, che ha comportato il trasferimento non autorizzato di 1,9 milioni di dollari. Un dipendente della società ha ricevuto via email una falsa comunicazione della Comerica Bank che lo invitava a seguire un link malevolo, aprendo il sito di phishing il dipendente ha provveduto a fornire le informazioni di accesso al conto corrente della società. Conseguentemente i criminali hanno avuto accesso ai conti correnti della Experi-Metal Inc. presso la Comerica Bank; nelle sei ore successive dai conti correnti sono stati effettuati 93 trasferimenti

---

[8] https://archive.is/V8u3Z#selection-561.0-639.479

[9] Tribunale di Milano, sentenza del 10.12.2007 – est. Gamacchio (Giudice per l'udienza preliminare): cfr. R. Flor, Frodi identitiarie e diritto penale, in Riv. giurisp. econ. az., 2008, 4, p. 184; A. Sorgato, Il reato informatico: alcuni casi pratici, in Giur. pen., 2008, 11, p. 40

[10] https://www.ilgiornale.it/news/ecco-noi-hacker-romeni-vi-svuotiamo-i-conti-bancari.html

[11] http://www.sophos.com/pressoffice/news/articles/2007/09/ameritrade.html

[12] https://en.wikipedia.org/wiki/Experi-Metal_v._Comerica

fraudolenti per un totale di 1.901.269,00 dollari. La maggior parte dei bonifici erano diretti a Russia, Estonia e Cina.

Nel Marzo 2011 la RSA Security[13], divisione della EMC Corporation, è rimasta vittima di un sofisticato attacco informatico finalizzato al furto di dati sensibili e di tipo APT (Advanced Persistent Threat). Per colpire la società è stata effettuata una campagna di spear phishing mediante l'invio di un documento di calcolo malevolo che sfruttava una vulnerabilità 0day di Adobe Flash (CVE-2011-0609). L'attacco ha sottratto alla società tutte le chiavi master dei token di sicurezza RSA SecureID; tali chiavi sono state successivamente sfruttate per compromettere diversi fornitori della difesa Americana[14].

Nell'Agosto del 2013 la società pubblicitaria Outbrain[15] ha subito un attacco di spear phishing da parte del collettivo Syrian Electronic Army, gli annunci pubblicitari gestiti da Outbrain presenti sulle principali testate giornalistiche americane come The Washington Post, Time, and CNN effettuavano un redirect dei visitatori verso alcuni siti gestiti dal collettivo.

Nel Novembre 2013 i dati personali e le carte di credito di 110milioni di utenti del colosso internazionale Target Brands, Inc.[16] sono stati sottratti tramite un attacco di spear phishing; la comunicazione malevola conteneva un malware.

Nel Dicembre del 2013 la campagna di phishing volta a distribuire il ransomware Cryptolocker aveva già infettato oltre 250mila computer[17]; la diffusione di ransomware è poi aumentata negli anni successivi fino a raggiungere gli oltre 181 milioni[18] di attacchi nel 2018.

Nel 2014 diversi personaggi famosi rimasero vittime di una campagna di phishing probabilmente mirata ai VIP che sfruttavano il servizio iCloud di Apple, l'attacco fu denominato "Fappening"[19] e ha visto la diffusione di immagini o video private di oltre 60 star.

---

[13] https://archive.is/rU2QS

[14] https://www.nytimes.com/2011/05/28/business/28hack.html

[15] https://www.theatlantic.com/international/archive/2013/08/syrian-hackers-use-outbrain-target-washington-post-time-and-cnn/312116/

[16] https://bringmethenews.com/news/report-email-phishing-scam-led-to-target-breach

[17] https://www.bbc.com/news/technology-25506020

[18] https://www.helpnetsecurity.com/2018/07/11/2018-sonicwall-cyber-threat-report/

[19] https://en.wikipedia.org/wiki/ICloud_leaks_of_celebrity_photos

A Maggio del 2014 è stato rilevato il primo attacco di SIM Swap[20], tale attacco ha l'obiettivo di aggirare l'autenticazione a due fattori se implementata sfruttando l'utenza telefonica. La frode sfrutta la capacità degli operatori di telefonia mobile di trasferire l'utenza telefonica di un abbonato su una differente scheda SIM; funzionalità normalmente sfruttata quando l'utente smarrisce o gli viene derubato il telefono cellulare. Il truffatore, dopo aver ottenuto le credenziali di accesso e i documenti della vittima tramite una campagna di phishing, eseguirà anche una sostituzione della scheda SIM ottenendo il pieno controllo dell'utenza telefonica e potrà quindi portare al termine l'attività illecita.

Nel Novembre 2014, in Italia, è stato rilevato il primo kit di phishing ai danni di un istituto di credito che prevede l'utilizzo di un Command and Control[21] per carpire non solo le credenziali di accesso ma anche il codice OTP in possesso agli utenti, e operare in tempo reale sul conto corrente delle vittime.

A Giugno 2015 il produttore di dispostivi di networking Ubiquiti Networks Inc.[22] ha subito un attacco di spear phishing che ha comportato un ammanco totale di 46,7 milioni di dollari, solo 8 milioni è riuscita successivamente a recuperare grazie alla cooperazione di alcuni istituti di credito. L'attacco è stato veicolato tramite false email che impersonavo comunicazioni dei dirigenti della società e richiedevano trasferimento di denaro.

Nel Febbraio 2016 la società aerospaziale austriaca FACC AG[23] è stata derubata di oltre 40 milioni di euro a causa di un attacco di phishing, che consisteva in una falsa email riportante come mittente il nominativo del CEO Walter Stephan, il quale richiedeva ad un dipendente il trasferimento di diverse somme di denaro verso un conto corrente dedicato al progetto, falso, di acquisizione di una società terza.

Nel 2017 una indagine della Polizia Postale Italiana[24] in collaborazione con la Guardia di Finanza, ha permesso di ricostruire una sofistica tecnica di Payout (l'operazione fisica di prelievo dei soldi frodati) mediante l'uso di voucher Inps. I criminali attraverso campagne di phishing ai danni degli utenti della carta di credito prepagata PostePay procedevano all'acquisto di voucher Inps; usualmente sfruttati per il pagamento di prestazioni occasionali, il valore dei voucher veniva poi rigirato su carte di credito prepagate denominate Poste Pay INPS Card e sfruttate per il prelievo in contate delle somme sottratte. L'operazione ha permesso ai criminali di sottrarre quasi due milioni

---

[20] https://www.actionfraud.police.uk/alert/alert-how-you-can-be-scammed-by-a-method-called-sim-splitting

[21] https://www.d3lab.net/phishing-con-c2-per-aggirare-i-token-otp/

[22] https://krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberheist/

[23] https://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF

[24] https://www.adnkronos.com/fatti/cronaca/2017/03/02/acquistavano-voucher-inps-illecitamente-centinaia-vittime-tutta-italia_iQRmZwju1JZhf0gqU5PgpM.html

di euro agli utenti e l'utilizzo della INPS Card permetteva di prelevare dagli ATM importi giornalieri maggiori a differenza di una normale carta PostePay, che invece ha massimali più bassi.

Sempre nel 2017 una nuova campagna di phishing ai danni di PayPal richiede all'utente non solo i dettagli del proprio account e i dati della carta di credito, ma anche di confermare la propria identità inviando un selfie[25] mentre tiene in mano un proprio documento di riconoscimento e la carta di credito. Questa tecnica non solo permette di avere una doppia verifica delle informazioni della carta di credito ma permette ai criminali di ottenere la foto di un documento di identità, utile per condurre un furto di identità.

A Luglio 2018, in Italia[26], è stata rilevata la prima campagna di phishing mediante l'uso di un falso Social Care sulla piattaforma Facebook. I criminali creavano false pagine o profili di Poste Italiane S.p.A. e contattavano direttamente tutti gli utenti di Poste che chiedevano informazioni o lamentavano disservizi nella pagina ufficiale. Gli utenti una volta contattati mediante il servizio di messaggistica istantanea Facebook Messenger venivano chiamati telefonicamente dai criminali per concludere la truffa ed ottenere dalla vittima ulteriori informazioni, come il codice OTP per convalidare dei pagamenti.

A febbraio del 2019 una sofistica campagna di phishing ha preso di mira gli utenti di Google[27] e sfruttato il servizio, legittimo, Google Translate per nascondere il sito malevolo. L'utente era infatti invitato a visitare il sito web translate.google.com il quale appariva fedelmente nella barra dell'indirizzo senza alcuna alterazione; quest'ultimo effettuava la traduzione di un sito di phishing e permetteva quindi alla vittima di inserire le proprie credenziali. L'utente conscio di essere su un dominio ufficiale di Google acconsentiva a fornire le proprie credenziali ignaro della tecnica sfruttata per nascondere il reale sito fraudolento.

[25] https://cofense.com/smile-new-paypal-phish-victims-sending-selfie/

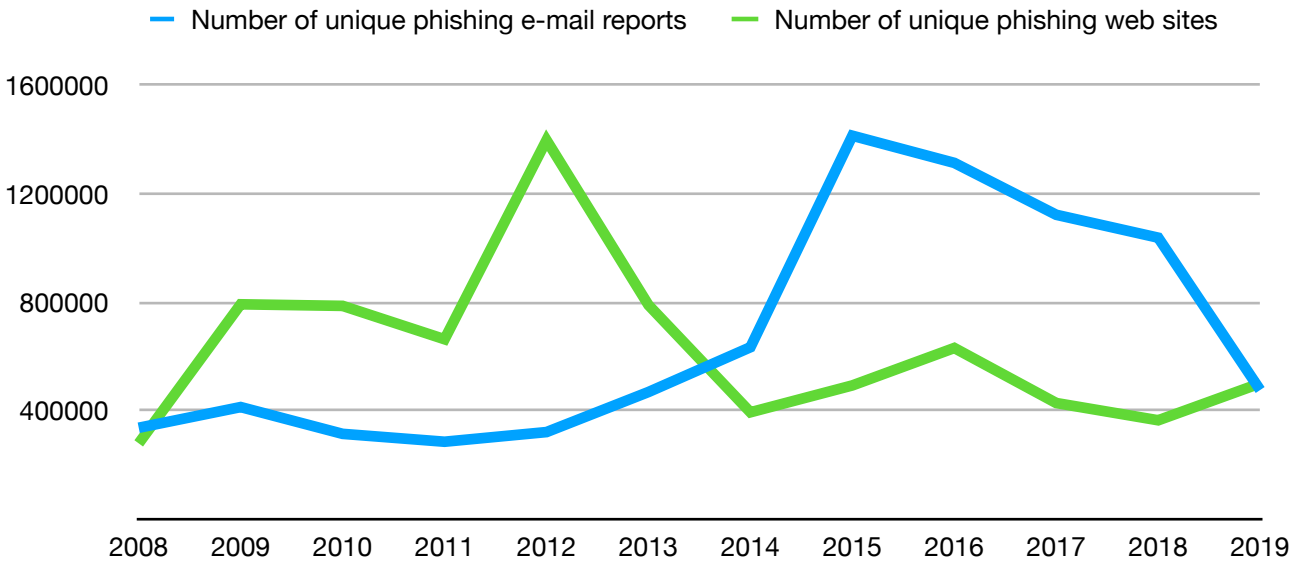
[26] https://www.d3lab.net/phishing-tramite-falso-social-care-ai-danni-degli-utenti-postepay/

[27] https://www.zdnet.com/article/hacker-group-uses-google-translate-to-hide-phishing-sites/

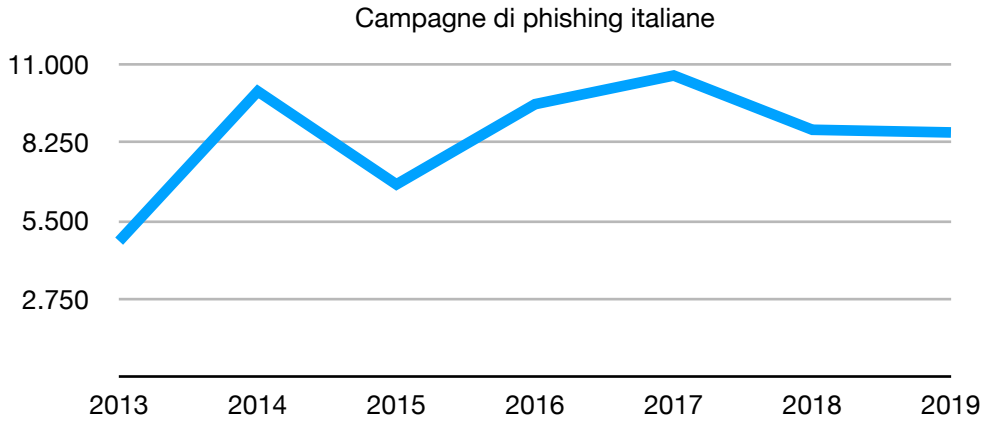
3. Statistiche

L'Anti-Phishing Working Group (APWG) rilascia ogni trimestre un report28 contenente il rapporto sulle attività di phishing analizzate riportando il numero univoco di email e il numero univoco dei siti malevoli rilevati; di seguito il grafico sull'andamento annuale delle campagne rilevate fino al 31 Dicembre 2019.

È presente un trend di decrescita delle campagne di phishing veicolate tramite le email negli ultimi cinque anni pur rimanendo costante il numero univoco di siti web malevoli; questo dato conferma che i criminali stanno sfruttando vettori di attacco differenti quali gli SMS o i Social Network.



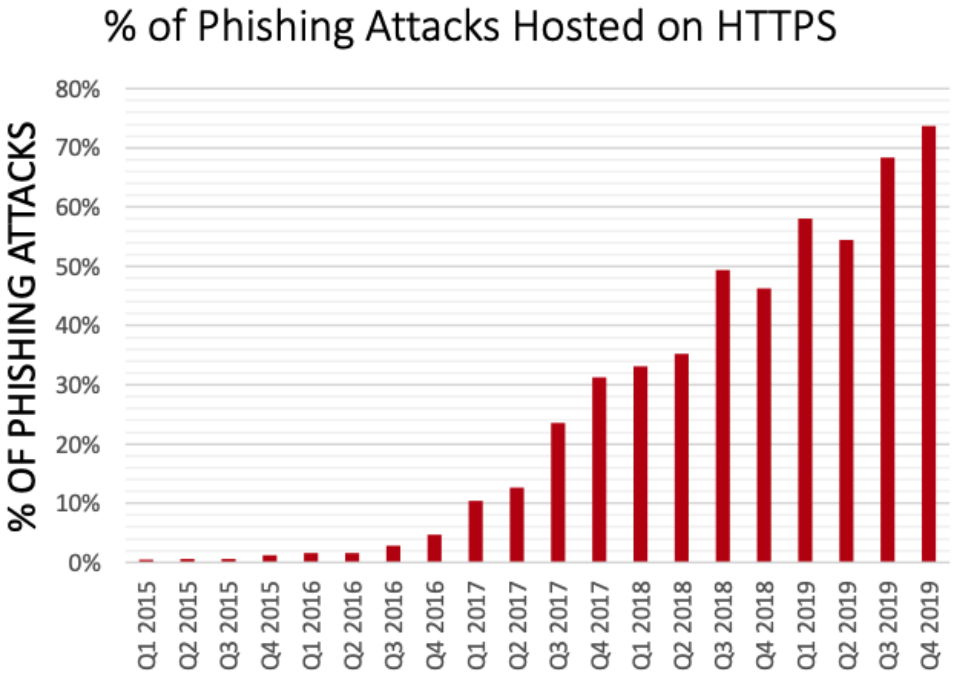
In ambito Italiano, i dati forniti da D3Lab[29], ci permettono di visualizzare le campagne di phishing univoche rilevate ai danni degli utenti italiani. L'andamento degli ultimi anni risulta costante in linea con i dati internazionali, con una media di 25 campagne di phishing giornaliere negli ultimi cinque anni.



[28] https://apwg.org/trendsreports/

[29] https://www.d3lab.net/

Una ricerca di PhishLabs[30] evidenzia come la qualità delle singole campagne sia aumentata; infatti quasi i tre quarti di tutti i siti di phishing ora utilizzano il protocollo HTTPS. È il dato più alto registrato dall'inizio del 2015, e conferma il fatto che che gli utenti non possono fare affidamento sul solo certificato SSL per capire se un sito è sicuro o meno.



Kaspersky Lab. ha pubblicato[31] le statistiche sullo Spam e sul phishing del 2019 in cui evidenzia diverse caratteristiche sulle loro attività di indagine.

Il 56,51% delle email inviate nel 2019 contengono spam; 4 punti percentuali in più rispetto al 2018. I principali paesi che hanno inviato email di spam sono la Cina (21,26%), gli USA (14,39%) e la Russia (5,21%).

Il paese al quale sono indirizzate il maggior numero di campagne malevoli è la Germania (11,86%), seguita dalla Russia e dal Vietnam entrambi alla medesima posizione (5,77%), l'Italia segue questi paesi ricevendo il 5,57% delle campagne di email malevoli.

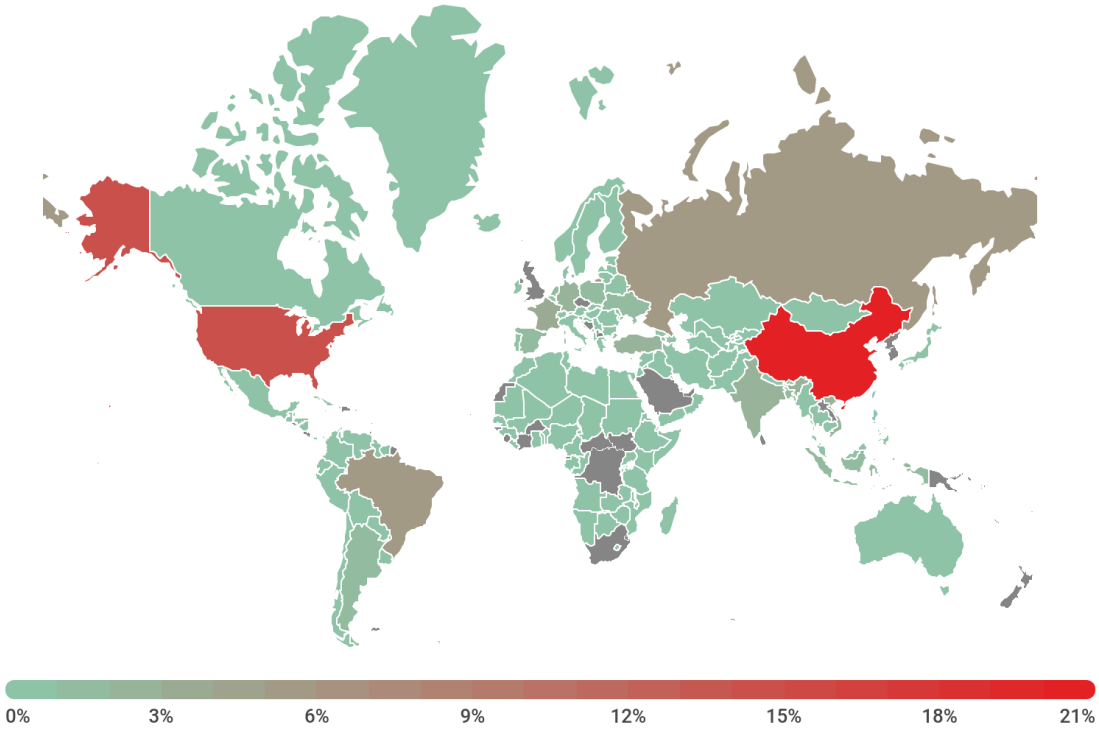
Più specificatamente per la sola categoria del phishing il Venezuela è il principale paese colpito con il 31,16% di utenti unici attaccati rispetto al numero totale della popolazione; il 20,17% degli Italiani ha anche esso ricevuto un attacco di phishing nel corso del 2019.

Le organizzazioni più colpite dal phishing sono gli Istituti di Credito (27,16%), seguiti dai provider di servizi web (21,12%) e successivamente dai circuiti di pagamento (16,67%).

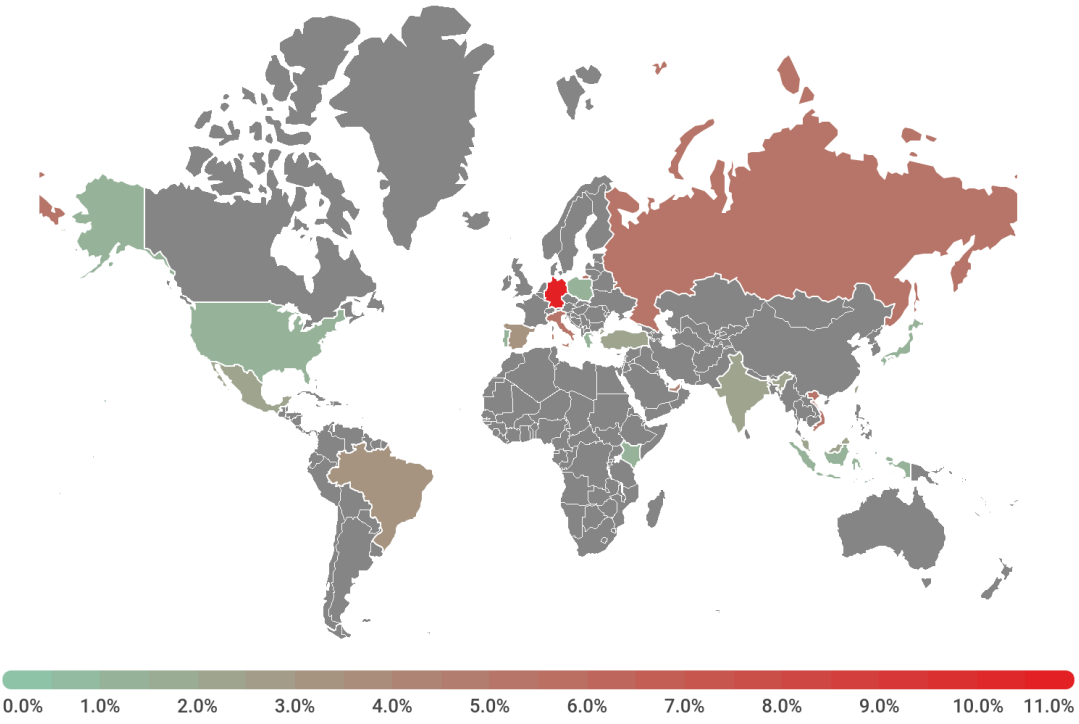
---

[30] https://info.phishlabs.com/blog/top-phishing-trends-2019

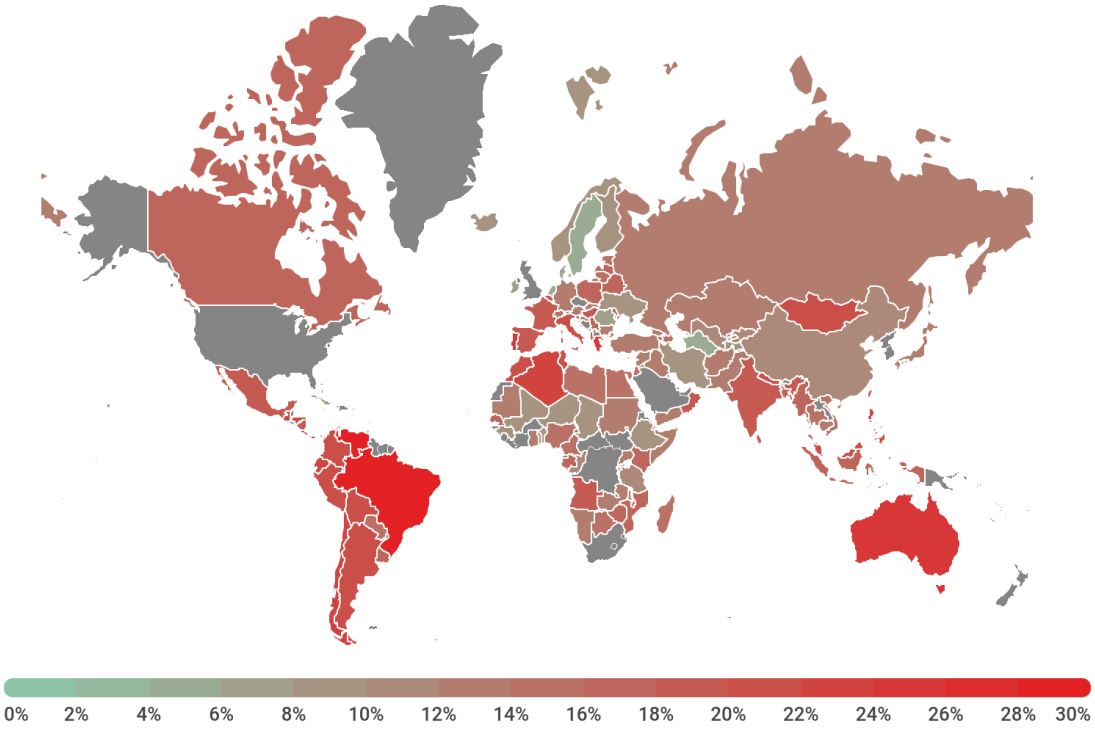
[31] https://securelist.com/spam-report-2019/96527/



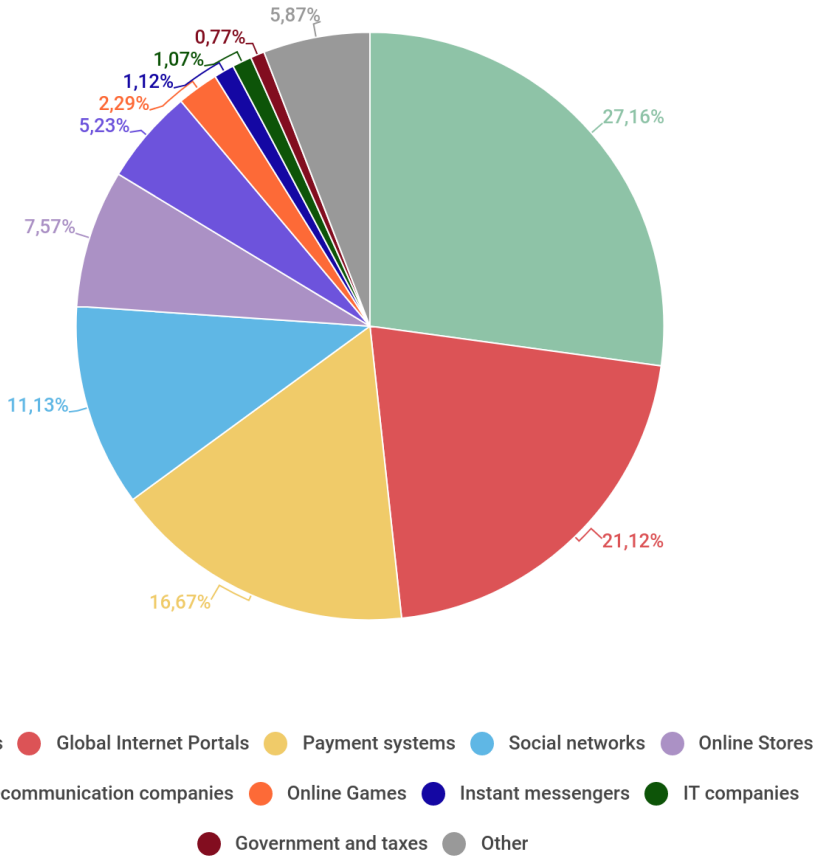
Sources of spam by country



Countries targeted by malicious mailings



Countries by share of attacked users



Rating of categories of organizations attacked by phishers

4. Tipologie di Attacchi

Sussistono diverse tipologie di attacchi, le quali si differiscono principalmente per metodica e target.

La tradizionale campagna di phishing viene effettuata su una ampia platea di utenti e senza una verifica accurata di esse con l'intento di acquisire il più grande numero di informazioni sensibili.

Una campagna di più accurata e mirata nei confronti di un individuo o una società è definita **Spear Phishing**; questa tipologia di attacchi prevede un'attenta analisi sul target e a volte vengono preceduti da una attività di OSINT[32] (Open Source INTelligence) per individuare quante più informazioni pubbliche esistono della vittima. Informazioni che spesso vengono sfruttate nella campagna malevola per rendere la comunicazione più attendibile ed incrementare il possibile successo dell'attacco.

Il **Clone Phishing** è un altra tipologia di attacco e consiste in una campagna che sfrutta una precedente comunicazione lecita, sostituendo i riferimenti del mittente con quelli dell'attaccante, e/o alcune parti della comunicazione; l'attaccante così facendo si assicura la fiducia del destinatario che riconosce una comunicazione già ricevuta in precedenza e si sostituisce al reale mittente per perfezionare l'attacco. Questa tipologia di attacco è anche denominata Man in the Email[33], una variazione del "Man in the Middle".

Il **Whaling** è una tipologia che identifica una campagna mirata verso figure di spicco all'interno di una società o della scena politica di un paese, ad esempio un CEO o il presidente di una maggioranza politica. L'attacco viene pianificato e creato su misura per l'obiettivo al fine di rendere la comunicazione più realistica possibile e garantendo un maggior successo all'attacco.

Esiste infine un ultima tipologia di attacco più avanzata denominata **BEC** (Business Email Compromise) in cui l'aggressore impersona una figura di rilievo all'interno di una società, come il CEO o il CFO. L'attaccante effettua pertanto comunicazioni per conto di tale figura sia all'interno della medesima società, richiedendo per esempio ad un dipendente di eseguire determinate azioni, o esternamente richiedendo ad esempio ad un fornitore di modificare precedenti accordi intercorsi.

---

[32] https://en.wikipedia.org/wiki/Open-source_intelligence

[33] https://archives.fbi.gov/archives/seattle/press-releases/2013/man-in-the-e-mail-fraud-could-victimize-area-businesses

5. Vettori

Ogni campagna di phishing deve essere in qualche maniera diffusa alle potenziali vittime, e può trattarsi di un attacco massivo a più soggetti o diretto ad un singolo target. La diffusione può avvenire con differenti strumenti a volte usati in abbinata per completare un attacco.

5.1 Mail

Le prime campagne di phishing sono state veicolate sfruttando la posta elettronica e la possibilità di alterare con estrema facilità il mittente di un messaggio email. Questa tecnica è detta spoofing e prevede la falsificazione del mittente della email con l'intento di impersonare qualcun altro all'interno di una comunicazione.

5.2 Short Message Service

Gli SMS (Short Message Service) sono un vettore di attacco più recente grazie ad una riduzione dei costi di invio dei messaggi e una più capillare diffusione di provider che permettono l'invio massivo di messaggi a diversi destinatari tramite una comoda interfaccia grafica sul web. Una campagna di phishing veicolata tramite i messaggi di testo è detta di Smishing (short message phishing).

Lo smishing utilizza i messaggi di testo per inviare l'attività di frode ed indurre le persone a divulgare le loro informazioni personali. Il messaggio solitamente riporta un sito web fraudolento molto simile all'originale sfruttando la tecnica di typosquatting. Tale similitudine ha l'intento di ingannare l'utente che non accorgendosi delle variazioni visiterà il sito pensando di trovarsi su quello ufficiale.

È infine possibile effettuare lo spoofing del mittente del messaggio, ovvero impersonare il nominativo o numero di telefono di un'altra persona o soggetto, avvalorando maggiormente la comunicazione.

5.3 Voice

Le chiamate vocali sono un ulteriore vettore di attacco per le campagne di phishing, il Vishing (voice phishing) fa leva sulla maggiore fiducia che l'essere umano tende a riporre in una persona con la quale si ha un dialogo telefonico.

Il vishing più precisamente è una attività di frode che utilizza l'ingegneria sociale tramite il sistema telefonico; i fatti del mondo reale hanno ampiamente dimostrato come una conversazione

telefonica migliori l'efficacia di un attacco in modo significativo[34]. Questo non accade normalmente con le email poiché devono essere lette e quindi lasciano meno possibilità agli aggressori di attirare le vittime.

Anche per il vishing è possibile sfruttare la tecnica di spoofing, l'id del chiamante può essere falsificato avvalorando maggiormente la comunicazione.

5.4 Social Network

I Social Network hanno raggiungo livelli di utilizzo e diffusione impensabili fino a qualche anno fa. Il Global Web Index[35] in una ricerca condotta nel 2019 ha raccolto i dati di utilizzo dei social network nei diversi continenti stabilendo una media di utilizzo per utente di 2h e 30minuti al giorno con oltre 2 miliardi di utenti attivi mensilmente nella piattaforma più diffusa, Facebook.

Data l'importante presenza di utenti nei Social Network i criminali hanno iniziato a sfruttare queste nuove piattaforme per divulgare le proprie attività di frode. Attraverso la creazione profili o pagine false è possibile diffondere una falsa comunicazione debita ad invitare gli utenti a visitare un sito di phishing in cui carpire informazioni sensibili delle vittime.

5.5 Instant Message

I servizi di messaggistica istantanea permettono agli utenti di scambiare velocemente brevi messaggi; grazie alla diffusione degli Smartphone ed ai costi di connettività sempre inferiori le piattaforme di Instant Message sono diventate sempre più popolari ed utilizzate. WhatsApp, l'applicazione maggiormente utilizzata, ha 2 miliardi di utenti registrati[36] di cui 500mila che la utilizzano giornalmente[37].

Vista la facilità e la velocità con cui è possibile scambiare brevi messaggi nelle piattaforme di Instant Messagge i criminali hanno iniziato a sfruttare queste tecnologie per divulgare le proprie attività di frode[38].

Data la consapevolezza diffusa tra gli utenti dei pericoli degli attacchi di phishing tradizionali veicolati tramite email è importante per i criminali sfruttare vettori di attacco nuovi e differenti, ottenendo quindi una maggior attenzione da parte dell'utente finale.

---

[34] http://home.deib.polimi.it/fmaggi/downloads/publications/2010_maggi_vishing.pdf

[35] https://www.visualcapitalist.com/visualizing-social-media-use-by-generation/

[36] https://blog.whatsapp.com/two-billion-users-connecting-the-world-privately

[37] https://www.statista.com/statistics/730306/whatsapp-status-dau/

[38] https://www.infosecurity-magazine.com/next-gen-infosec/whatsapp-attack-mobile-phishing/

5.6 Advertising

L'utilizzo di inserzioni pubblicitarie[39] ha permesso di portare le campagne di phishing ad un livello ancora più alto, in quanto l'attaccante è in grado di veicolare la frode sfruttando gli strumenti di targetizzazione offerti dalle piattaforme pubblicitarie.

Gli strumenti di targetizzazione, o anche targeting, sono in grado di individuare il pubblico interessato ad un prodotto o servizio tra gli utenti del sito web visitato. Tali strumenti permettono di realizzare campagne di phishing indirizzate esclusivamente agli utenti che sfruttano un determinato servizio, di una determinata area geografica o di una fascia di età prestabilita.

[39] https://blog.kraken.com/post/225/kraken-phishing-warning/

6. Dissimulare

Le campagne di phishing devono trasmettere un senso di sicurezza all'utente finale, facendogli credere di aver ricevuto una comunicazione ufficiale. È quindi importante per i criminali sfruttare ogni possibile strumento per riprodurre la medesima esperienza che l'utente avrebbe in una comunicazione lecita.

6.1 Grafica

Usualmente le campagne di phishing ripropongono l'interfaccia grafica di un sito web noto al fine di convincere la vittima di trovarsi sul sito originale e non un portale di phishing. È importante per il criminale riprodurre fedelmente il sito originale offrendo alla vittima la medesima esperienza di navigazione.

È possibile riprodurre il sito originale avvalendosi di strumenti che permettono di scaricare localmente un intero sito web, come Httrack[40] che è una applicazione Open Source sviluppata per creare il mirroring locale di un sito web.

Ottenuta una copia locale del sito web originale il criminale apporterà le minime e necessarie modifiche al fine di carpire le informazioni sensibili digitate dall'utente producendo un "Kit di phishing".

Il kit verrà pubblicato online e le vittime saranno invitate a visitarlo mediante una comunicazione fraudolenta.

6.2 Multilingue

L'esperienza di navigazione su un sito di phishing è fondamentale per poter carpire l'attenzione di una probabile vittima, pertanto è opportuno che le pagine web fraudolente siano realizzate usando il medesimo linguaggio degli utenti.

Alcuni kit di phishing per risultare più versatili e pertanto adeguati ad una più ampia platea di vittime sono stati sviluppati in multilingue, ovvero in grado di adattarsi alla lingua parlata dalla vittima. Questo è possibile verificando l'IP di provenienza dell'utente o il linguaggio impostato dal dispositivo in uso.

Questa tecnica è ampiamente sfruttata in campagne di phishing ai danni di enti internazionali i quali hanno clienti in diversi paesi del mondo e quindi che parlano differenti lingue.

[40] https://www.httrack.com

6.3 HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer) è un protocollo per rendere sicure le comunicazioni in un network di computer ed è ampiamente utilizzato su internet negli ultimi anni. In HTTPS, il protocollo di comunicazione è crittografato utilizzando Transport Layer Security (TLS) o, in precedenza, Secure Sockets Layer (SSL).

HTTPS fornisce una cifratura bidirezionale delle comunicazione tra un client e il server, cifratura che permette all'utente finale una maggior sicurezza e protegge ogni comunicazione da attacchi informatici come Man In The Middle, Tampering e Eavesdropping.

Accedendo ad un sito web da un comune browser si può identificare l'utilizzo del protocollo HTTPS grazie alla presenza di un lucchetto chiuso presente nella barra dell'indirizzo. Questa rappresentazione grafica permette sempre di verificare velocemente se la connessione con il sito web visitato è protetta da cifratura.

Purtroppo, anche a causa di errate campagne informative, molte persone pensano che le connessioni HTTPS siano anche indice di un sito sicuro e legittimo. Invece tale protocollo viene utilizzato sempre più su siti dannosi, sopratutto quelli di phishing.

Il protocollo HTTPS garantisce la sicurezza della connessione tra il client e il server, ma non garantisce i contenuti del sito web. Una pagina di phishing può quindi possedere il lucchetto.

Ad oggi il 70% dei siti di phishing sfrutta HTTPS[41]; i certificati vengono rilasciati gratuitamente e permettono al criminale di offrire all'utente finale una maggior fiducia grazie alla errata credenza che il lucchetto simboleggi l'affidabilità del sito web visitato.

6.4 Data URI Scheme

Le campagne di phishing potrebbero sfruttare la codifica base64 implementata nei principali browser tramite lo schema URI per offuscare la pagina di destinazione malevola.

Lo schema URI[42] permette di mostrare contenuti come se fossero risorse esterne. È una funzionalità supportata dai principali browser e sfruttata normalmente per incorporare immagini in un singolo file HTML, ma supporta qualsiasi contenuto web purché sia codificato in base64.

Base64 è uno schema di codifica che consente la rappresentazione di dati binari in stringhe di testo ASCII.

---

[41] https://info.phishlabs.com/blog/top-phishing-trends-2019

[42] https://en.wikipedia.org/wiki/Data_URI_scheme

La sintassi degli URI è stata definita nella RFC 2397[43] ed è costituita da:

data:[<media type>][;base64],<data>

Il <media type> specifica la tipologia di risorsa che il browser dovrà interpretare; è possibile specificare più tipologie di risorse separandole da un punto e virgola. Se il contenuto è codificato in base64 andrà riportato tramite il valore *;base64* e infine va specificato il dato da interpretare. Se non specificata la codifica in base64 il browser interpreterà il dato sfruttando la codifica ASCII.

Il phisher[44] potrà quindi sviluppare una pagina malevola, codificarla in base64 e indirizzare l'utente a tale risorsa. Questa nidificazione URI mostrerà nella barra dell'indirizzo il codice in base64 come codice HTML e pertanto visualizzerà alla vittima una pagina di phishing.

Per avvalorare maggiormente la campagna malevola e confondere la vittima è possibile sfruttare l'opzione di specificare più media type, inserendo un tipo di dato fittizio riportante il sito web oggetto della campagna di phishing. La vittima vedrà quindi il nella barra dell'indirizzo del proprio browser citato il sito web ufficiale avvalorando maggiormente l'ipotesi che stia visitando un sito legittimo e non di phishing.

Di seguito un data URI che mostrerà all'utente una pagina HTML contenente il testo "Hello World" e che indica un secondo tipo di dato fittizio riportante un sito ufficiale di esempio:

data:text/html;https://exampleofficialsite.com/verify/your/account/;base64,IDwhRE9DVFlQRSBodG1sPgo8aHRtbD4KPGhlYWQ+Cjx0aXRsZT5QYWdlIFRpdGxlPC90aXRsZT4KPC9oZWFkPgo8Ym9keT4KSGVsbG8gV29ybGQKPC9ib2R5Pgo8L2h0bWw+IA==

[43] https://tools.ietf.org/html/rfc2397

[44] https://www.proofpoint.com/sites/default/files/proofpoint-obfuscation-techniques-phishing-attacks-threat-insight-en-v1.pdf

6.5 Typosquatting

Il typosquatting, acronimo di typo “errore di battitura” e squatting “occupazione abusiva”, è una attività che mira a registrare domini civetta; ovvero domini che variano nel nome di pochi caratteri rispetto a quelli ufficiali e pertanto ad una prima vista l’utente finale potrebbe confonderli.

Un dominio che si basa sul typosquatting viene creato sfruttando possibili errori di battitura o lettere simili in altri alfabeti. Il risultato è sempre un sito molto simile all’originale; considerando example.com come sito web originale di seguito le possibile tecniche di variazione:

- Un errore di ortografia o spelling (anche in una differente lingua): exampple.com;
- Un errore di battitura: examlpe.com;
- Riformulazione del dominio: examples.com;
- Estensione (TLD) differente dall’originale: example.org;
- Estensione (TLD) con un carattere in meno o in più: example.co;
- Utilizzo di caratteri simili (Il numero uno anziché la elle): examp1e.com;
- Utilizzo di omofoni, parole simili che hanno un significato differente;
- Utilizzo della codifica Unicode (Punycode): exaмple.com.

Esistono diversi motivi[45] per cui i typosquatters (coloro che registrano domini basati sul typosquatting) creano tali domini:

- Per provare a rivendere il dominio al proprietario del dominio ufficiale;
- Monetizzare tramite pubblicità presente sul dominio visualizzata da utenti che sbagliano a digitare il sito;
- Reindirizzare i visitatori al sito web di un concorrente;
- Reindirizzare i visitatori verso il dominio ufficiale ma introducendo link di affiliazioni, qualora sia previsto un programma di affiliazione dal sito ufficiale;
- Creare un sito di phishing per raccogliere informazioni sensibili riproducendo il sito ufficiale;
- Veicolare l’installazione di Malware o Adware;
- Ricevere comunicazioni di posta elettronica da utenti che sbagliano a digitare il dominio;
- Pubblicare informazioni o opinioni differenti rispetto al dominio ufficiale.

Il typosquatting è una tecnica sempre più sfruttata in ambito di phishing soprattutto per le comunicazioni veicolate tramite SMS (smishing), poiché l’utente leggendo velocemente il messaggio, difficilmente riconosce ad una prima lettura un dominio creato con tale tecnica, ed è portato così a visitare il sito e fornire i dati sensibili come se si trovasse sul sito ufficiale.

[45] https://en.wikipedia.org/wiki/Typosquatting

6.6 Punycode

Punycode è la codifica Unicode, definita nella RFC 3492[46], per i nomi di dominio internazionalizzati (IDNA) tramite una sequenza di caratteri ASCII. L'implementazione ha premesso l'utilizzo di una sequenza di caratteri Unicode nel nome del dominio, senza dover modificare infrastrutture e standard esistenti. La successiva traduzione e rappresentazione grafica nella codifica originaria è demandata all'user agent utilizzato.

I nomi di domini creati con la codifica Punycode possono sembrare uguali a occhio nudo ai domini privi di tale codifica, ma in realtà hanno un indirizzo web differente. Alcune lettere dell'alfabeto romano, utilizzato dalla maggior parte delle lingue moderne, hanno una forma molto similare a quella delle lettere greche, cirilliche o altri alfabeti; quindi è facile per un aggressore registrare un nome di dominio che sostituisca alcuni caratteri tradizionali con caratteri Unicode. Ad esempio è possibile scambiare una t normale con un Tau greco τ, ad una prima lettura l'utente non noterebbe la differenza. In realtà tale carattere viene rappresentato dalla sequenza di caratteri ASCII: *n--5xa*.

Questa tecnica può essere sfruttata per diffondere domini di phishing che ad una veloce lettura potrebbero apparire legittimi, ma in realtà conducono la vittima ad un sito web appositamente creato per carpire informazioni sensibili.

[46] https://tools.ietf.org/html/rfc3492

7. Contrasto

Seppure con le limitazioni e i metodi di evasione che verrano in seguito descritti è importante segnalare e contrastare le campagne di phishing affinché gli utenti meno avvezzi alla tecnologia possano evitare una frode.

7.1 Blocklist

La blocklist, o blacklist, è una lista sfruttata per la verifica degli accessi, basata su diversi elementi (email, url, ip, nomi di dominio, ecc.). L'accesso alla risorsa richiesta è sempre consentito ad eccezione degli elementi presenti nella lista a cui viene negato l'accesso. L'opposto è una whitelist, dove solo gli elementi presenti nella lista hanno accesso alla risorsa; infine esistono le greylist che contengono elementi temporaneamente bloccati o consentiti.

Per contrastare il phishing esistono diverse blocklist a cui segnalare url malevoli; PhishTank[47] è una piattaforma comunitaria open source lanciata nel 2006 che raccoglie url di phishing e a seguito di una verifica manuale delle segnalazioni, per evitare falsi positivi, include tali url nella propria blocklist diffusa gratuitamente e aggiornata in tempo reale. È una piattaforma comunitaria poiché gli utenti possono segnalare nuovi url ma possono anche votare positivamente o negativamente segnalazioni effettuate da altri; una valutazione positiva conferma la presenza di materiale malevolo nell'url indicato, al contrario una votazione negativa sancisce la presenza di materiale lecito.

Google[48] permette di segnalare url malevoli, tali url non vengono verificati dalla comunità a differenza di PhishTank ma vengono verificati direttamente da Google anche grazie a tecniche di Machine Learning. Google non rilascia una blocklist pubblica ma sfrutta tali indicazioni per bloccare gli url malevoli grazie al servizio di Google Safe Browsing sfruttato dai principali browser per dispostivi mobile o desktop in grado di avvisare un utente con un banner rosso qualora stia effettuando l'accesso ad un sito di phishing.

Altri enti che permettono di ricevere segnalazioni di url di phishing sono:

- Microsoft[49], che sfrutta i dati a tutela degli utenti del proprio sistema operativo Windows;
- Netcraft[50], che utilizza i dati per proteggere la navigazione degli utenti che sfruttano la loro estensione per i principali browser;
- Symantec e altri principali antivirus che offrono sempre soluzioni di protezione ai loro clienti.

---

[47] https://www.phishtank.com/

[48] https://safebrowsing.google.com/safebrowsing/report_phish/?hl=it

[49] https://www.microsoft.com/en-us/wdsi/support/report-unsafe-site-guest

[50] https://report.netcraft.com/report

Le blocklist hanno pertanto il compito di bloccare gli utenti che inconsciamente stanno accedendo ad un url malevolo; l'utilizzo di una piattaforma comunitaria come PhishTank permette di ridurre l'efficacia delle tecniche di evasione in precedenza descritte, poiché non è una sola organizzazione ad effettuare la verifica, ma molteplici utenti in ogni paese del mondo.

7.2 RBL

Le RBL (Real-time Blackhole List) o Domain Name System-based Blackhole List (DNSBL) sono delle liste di indirizzi IP che vengono utilizzati per inviare, tramite email, spam, malware o phishing. La maggior parte dei software installati nei server di posta elettronica può essere configurata per sfruttare queste liste e rifiutare o contrassegnare tutti i messaggi provenienti da un indirizzo IP presente in tali elenchi.

Le RBL maggiormente usate sono quelle fornite da Spamhaus[51], Spamcop[52], Sorbs[53], BarracudaCentral[54] e Abuseat[55]. Analizzando l'header della email di phishing è possibile identificare l'IP mittente della comunicazione e segnalarlo alle RBL elencate così che possano bloccare future comunicazioni. È possibile eseguire manualmente l'identificazione dell'IP visionando il sorgente della email oppure avvalendosi di strumenti online che effettuano un'analisi automatica del sorgente. MXToolBox Email Header Analyzer[56] e Meioc (Mail Extractor IoC)[57] sono due validi strumenti che permettono un analisi automatica.

Nel contrasto al phishing l'utilizzo di queste liste permette di segnalare gli IP dei server mail che stanno inviando comunicazioni malevoli e il server di posta elettronica del ricevente verificherà tali indicatori segnalando l'email come indesiderata, diminuendo così la probabilità che l'utente finale la riceva o la legga.

---

[51] https://www.spamhaus.org/

[52] https://www.spamcop.net/

[53] http://www.sorbs.net/

[54] https://barracudacentral.org/

[55] https://www.abuseat.org/

[56] https://mxtoolbox.com/EmailHeaders.aspx

[57] https://meioc.org

7.3 Abuse Team

Ogni provider ha al suo interno un organo competente per analizzare e individuare attività sospette o illecite che stanno avvenendo nella propria infrastruttura; tale organo è denominato Abuse Team.

È possibile quindi da parte di estranei segnalare agli Abuse Team dei provider coinvolti nella campagna di phishing l'utilizzo illecito dei servizi da loro offerti; compatibilmente con la legislatura vigente nel paese di ubicazione del provider, verranno prese le opportune decisioni per disabilitare la campagna malevola.

8. Blocklist e Tecniche di Evasione

Con l'obiettivo di proteggere gli utenti finali, diversi browser hanno introdotto la funzionalità di navigazione sicura (Safe Browsing); tale funzionalità mostra all'utente un avviso qualora tentasse di accedere ad un url malevolo. Tutti i servizi di Safe Browsing esistenti impediscono l'accesso ad un url malevolo facendo affidamento ad una blocklist dinamica, contenente l'elenco degli url di phishing.

La principale blocklist attualmente in uso dai Browser Chrome, Chromium, Firefox e Safari che detengono una quota di mercato superiore al 65% é generata da Google e denominata Google Safe Browsing. Internet Explorer ed Edge sfruttano invece il servizio Microsoft SmartScreen, ed infine altri browser minori sfruttano un servizio offerto da Yandex. Esistono inoltre altre blocklist come Web of Trust (WOT), NortonSafe Web e McAfee SiteAdvisor.

Ogni servizio di blocklist prevede una convalida dell'url malevolo che può essere segnalato dall'utente o identificato mediante procedure di Thread Intelligence; la procedura di convalida è un'operazione fondamentale per evitare la generazione di falsi positivi e pertanto bloccare l'accesso a siti web leciti.

Dopo aver convalidato l'utilizzo malevolo di una risorsa web, Google procede a generare un hash SHA-256 dell'url[58]; tale hash viene incluso in un database pubblico per i soli primi 32 bits che i browser in precedenza menzionati acquisiscono automaticamente e ripetutamente durante la sessione di navigazione di un utente. Quando un utente visita un sito web, automaticamente il browser genera un hash SHA-256 dell'url digitato; se i primi 32 bits dell'hash generato corrispondono ad un hash nel database di Google il browser interrogherà le API di Google verificando se l'intero hash coincide o meno.

Qualora i due hash dovessero corrispondere, all'utente finale verrà mostrato un messaggio di avviso, usualmente su sfondo rosso, che lo avvisa della presenza di un contenuto malevolo sul sito che si vorrebbe visitare.

La funzione hash è una funzione non invertibile che data una stringa in input A di lunghezza arbitraria produce una stringa B di lunghezza costante. Pertanto al variare dell'url verrà prodotto un hash di lunghezza costante sempre differente.

Data la cardinale operazione di convalida degli url malevoli e l'ampia diffusione dello strumento di Safe Browsing, è fondamentale per i criminali implementare tecniche di evasione che gli permettano di evitare l'indicizzazione della pagina web malevola nelle blocklist.

---

[58] https://www.inrialpes.fr/planete/people/amkumar/papers/gsb-security.pdf

8.1 Geo-blocking

Il geo-blocking è possibile introducendo la verifica della geolocalizzazione dell'utente che visita il sito di phishing.

La geolocalizzazione permette al phisher di identificare il paese di provenienza della vittima; tale verifica viene usualmente fatta mediante l'IP o la lingua del browser che l'utente usa per la navigazione sul web. Se l'utente proviene da un paese non target per la campagna di phishing generalmente viene reindirizzato verso un sito con contenuti leciti. Ciò può includere pagine false (Es. 404 Not Found, 403 Unauthorized, account sospeso, pagina bianca, ecc), il sito web legittimo del brand oggetto di abuso, siti pubblicitari, siti per adulti o anche solo una pagina bianca[59].

Questa tecnica permette di limitare l'efficacia delle blocklist poiché i soggetti verificatori potrebbero accedere al sito di phishing da un'area non destinataria nella campagna malevola e quindi non vedendo il contenuto malevolo non riescono a certificarne l'utilizzo fraudolento.

Di seguito si riporta un esempio di codice sfruttato dai phisher per identificare la provenienza; se l'utente proviene dall'Europa verrà indirizzato al sito malevolo altrimenti sul sito ufficiale di Google.

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.4.1/jquery.min.js"></script>
<script>
        $.getJSON('https://api.ip.sb/geoip?callback=?', function (data) {
                if (data.continent_code == "EU"){
                        $(location).attr('href', 'http://example.xsph.ru/phishing-page/')}
                else {
                        $(location).attr('href', 'https://google.it/')}
        });
</script>
```

8.2 IP Blocking

L'identificazione dell'IP permette all'attaccante non solo di definire la provenienza della vittima, ma anche l'Internet Service Provider (ISP) in uso e di creare regole di filtraggio dedicate. Il phisher potrà quindi impedire l'accesso a determinati indirizzi IP appartenenti ai soggetti che hanno il compito di analizzare e segnalare il phishing. Se l'IP appartiene alla lista degli indirizzi da bloccare viene indirizzato su un sito con contenuti leciti. Ciò può includere pagine false (Es. 404 Not Found, 403 Unauthorized, account sospeso, pagina bianca, ecc), il sito web legittimo del brand oggetto di abuso, siti pubblicitari, siti per adulti o anche solo una pagina bianca.

[59] https://info.phishlabs.com/blog/phishing-blocking-techniques-geoblocking-ip

Di seguito si riporta un esempio di codice sfruttato dai phisher con l'intento di bloccare gli IP dei soggetti verificatori:

```
$ips = array("^66.211.160.86*", "^46.244.*.*", "^131.*.*.*", "^157.*.*.*", ..,);

foreach($ips as $ip) {
 if(preg_match('/' . $ip . '/',$_SERVER['REMOTE_ADDR'])){
        header("HTTP/1.0 404 Not Found");
        die("<h1>404 Not Found</h1>The page that you have requested could not be found.");
 }
}
```

8.3 Hostname Blocking

L'hostname è il nome identificativo di un dispositivo collegato a una rete e utilizzato per identificarlo durante le comunicazioni. I nomi host possono essere nomi semplici costituiti da una singola parola o frase, oppure possono essere strutturati. RFC1034[60] indica che l'hostname può essere composta da più parti separate da punti, ogni parte può contenere al massimo 63 caratteri e il nome complessivo non deve superare i 255 caratteri.

L'hostname permette al phisher di effettuare un'ulteriore verifica della tipologia dell'utente che visita il sito di phishing. Se il dispositivo che effettua un accesso al sito malevolo è di uno dei soggetti verificatori gli verrà impedito l'accesso, così che il sito web non possa essere identificato come malevolo. Se l'hostname appartiene alla lista degli indirizzi da bloccare viene indirizzato su un sito con contenuti leciti. Ciò può includere pagine false (Es. 404 Not Found, 403 Unauthorized, account sospeso, pagina bianca, ecc), il sito web legittimo del brand oggetto di abuso, siti pubblicitari, siti per adulti o anche solo una pagina bianca.

Di seguito si riporta un esempio di codice sfruttato dai phisher con l'intento di bloccare gli hostname dei soggetti verificatori:

```
$blocked_hostname = array( "google", "phishtank", "norton", "yandex", ...);

foreach($blocked_hostname as $word) {
   if (substr_count(gethostbyaddr($_SERVER['REMOTE_ADDR']), $word) > 0) {
        header("HTTP/1.0 404 Not Found");
        die("<h1>404 Not Found</h1>The page that you have requested could not be found.");
   }
}
```

[60] https://tools.ietf.org/html/rfc1034

8.4 User-Agent Blocking

L'user-agent è un software che agisce per conto dell'utente, come il browser web che permette la visualizzazione e il rendering di un contenuto online, o come il client di posta elettronica che permette una facile lettura della propria messaggistica. Quando un utente visita un sito web una stringa di testo contenente le informazioni dell'user-agent viene inviata al server remoto.
Questa informazione permette usualmente di ricevere dal server i contenuti appropriati per il dispositivo e software in uso, se si utilizza ad esempio uno smartphone si visualizzerà un sito web ottimizzato per la navigazione mobile, differentemente se si utilizza un computer desktop.

L'user-agent è anche sfruttato dai bot per specificare la tipologia di servizio automatico che sta visitando il sito web, ad esempio il motore di ricerca Google sfrutta un identificativo specifico per indicare l'indicizzazione dei contenuti di un sito internet.

I phisher hanno introdotto[61] una verifica dell'user-agent per escludere l'accesso ad eventuali bot o sistemi automatici che hanno il compito di convalidare il contenuto malevolo. Inoltre visto il crescente numero di attacchi rivolti ai soli dispositivi mobile viene effettuato un ulteriore filtraggio impedendo l'accesso a dispositivi desktop.

Pertanto se l'user-agent del soggetto verificatore o dell'utente non corrisponde al target prestabilito dal phisher si viene indirizzati su un sito con contenuti leciti limitando l'efficacia delle blocklist.

Di seguito si riporta un esempio di codice sfruttato dai phisher con l'intento di bloccare l'user-agent di Google e PhishTank:

```
$useragent = $_SERVER['HTTP_USER_AGENT'];
if (strpos($useragent, "google") OR strpos($useragent, "phishtank") !== false ) {
        header("HTTP/1.0 404 Not Found");
        die("<h1>404 Not Found</h1>The page that you have requested could not be found.");
}
```

Di seguito si riporta un esempio di codice sfruttato dai phisher con l'intento di bloccare l'accesso a tutti gli utenti che non sfruttano uno specifico dispositivo (iPhone):

```
$useragent = $_SERVER['HTTP_USER_AGENT'];
if (strstr($useragent, "iPhone") === false ) {
        header("HTTP/1.0 404 Not Found");
        die("<h1>404 Not Found</h1>The page that you have requested could not be found.");
}
```

[61] https://info.phishlabs.com/blog/evasion-techniques-user-agent-blocking

8.5 Random Path

Un'altra tecnica implementata per vanificare il funzionamento delle blocklist è la generazione di parti randomiche all'interno di un URL di phishing. Generando ad esempio sottodomini, o sottodirectory random ad ogni accesso al sito di phishing, l'url che l'utente visiterà non sarà mai univoco ma in costante variazione. Questa continua variazione non permette di identificare l'url malevolo e quindi si limita l'efficacia delle blocklist.

Il phisher quindi, producendo url sempre differenti produrrà degli hash diversi tra loro che non troveranno alcun riscontro nelle blocklist, invalidando così la funzione di Safe Browsing in precedenza descritta.

Usualmente vengono introdotte parti randomiche nell'url attraverso i sottodomini (sfruttando la funzione di wildcard delle zone DNS) o con directory create Ad Hoc.

Di seguito si riporta un esempio di codice sfruttato dai phisher con l'intento di generare directory random:

```
function recurse_copy($src,$dst) {
    $dir = opendir($src);
    @mkdir($dst);
    while(false !== ( $file = readdir($dir)) ) {
        if (( $file != '.' ) && ( $file != '..' )) {
            if ( is_dir($src . '/' . $file) ) {
                recurse_copy($src . '/' . $file,$dst . '/' . $file);
            }
            else {
                copy($src . '/' . $file,$dst . '/' . $file);
            }
        }
    }
    closedir($dir);
}

$random=rand(0,100000000000);
$md5=md5($random);
$dst=base64_encode($md5);

recurse_copy("Original", $dst );
```

9. Filtri Anti-spam e Tecniche di Evasione

Le caselle di posta elettronica si sono dotate progressivamente negli ultimi anni di un servizio di anti-spam in grado di rilevare e segnalare all'utente finale tutte le comunicazioni indesiderate; ovvero le email che contengono campagne pubblicitarie aggressive, comunicazioni di phishing o divulgano campagne malware (Malspam).

Usualmente i filtri anti-spam sfruttano diverse tecniche per identificare i messaggi indesiderati, di seguito i filtri più noti.

Il filtro bayesiano[62] è una tecnica statistica di filtraggio della posta elettronica in uso dal 1996 e analizza tutti gli elementi di una email come indirizzo e nome del mittente, dominio email del mittente, parole contenute nel testo o nell'oggetto, immagini, link e allegati alla ricerca di parole chiave o combinazioni sospette.

I filtri possono essere, inoltre, basati su criteri euristici in grado di calcolare automaticamente le probabilità che una mail sia sospetta sulla base di un confronto con precedenti comunicazioni ricevute nella casella di posta elettronica nelle quali si riscontrano sia similitudini ma anche evidenti e parziali differenze.

Il checksum fuzzy è un ulteriore filtro e sfrutta una tecnica sviluppata per identificare i messaggi indesiderati, il contenuto dello spam può spesso variare nei dettagli (es. testo personalizzato per ogni destinatario) il che renderebbe inefficace un normale checksum. Il checksum fuzzy riduce il corpo del testo al suo minimo caratteristico e quindi ne genera un checksum. Questa riduzione del corpo del testo al suo minimo aumenta le possibilità che differenti email di spam riproducano lo stesso checksum e quindi aumenta la possibilità di identificazione di tali messaggi.

I filtri in precedenza descritti assegnando un punteggio ad ogni email analizzata; maggiore è il punteggio assegnato maggiore è la probabilità che il messaggio ricevuto sia indesiderato.

Apache SpamAssassin è il software anti-spam open source maggiormente diffuso ed utilizza molteplice tecniche per il rilevamento dello SPAM, filtro bayesiano, checksum fuzzy, Real-time Blackhole List (RBL), Blocklist e verifica DNS. SpamAssassin attribuisce un punteggio ad ogni email se il punteggio è superiore a 5.0 il messaggio probabilmente è indesiderato.

Risulta pertanto importante per un phisher eludere i filtri ed ottenere bassi punteggi al fine di garantire la ricezione del messaggio malevolo.

---

[62] https://en.wikipedia.org/wiki/Naive_Bayes_spam_filtering

9.1 Allowed URL

I filtri anti-spam, come SpamAssassin[63], analizzano il testo della email individuando la presenza di eventuali url. Per ogni url individuato viene estratto solamente il dominio e verificata la sua presenza su eventuali blocklist.

Se il dominio risulta presente nelle blocklist il filtro anti-spam andrà ad aumentare il punteggio assegnato al messaggio con la conseguente probabilità di contrassegnarlo come indesiderato.

Per garantirsi una capillare comunicazione del messaggio malevolo ed evitare che venga contrassegnato come indesiderato, il phisher deve sfruttare domini che non sono presenti nelle blocklist o di grande diffusione e autorevolezza, come i domini che risultano nelle liste bianche (whitelist) e non possono quindi essere presenti nelle blocklist.

Le Whitelist sono liste contenenti domini di grande utilizzo che non possono essere bloccati poiché sfruttati da una larga scala di utenti del web. Ad esempio contengono i domini di Google, Amazon, Facebook, Twitter e tanti altri servizi tra i più diffusi. Il sevizio Alexa Rank[64] offerto da Amazon aggiorna periodicamente la lista di tali domini e divulga una lista contenente un milione di siti maggiormente visitati.

I phisher dovranno quindi includere nelle loro comunicazioni malevoli, per quanto possibile, dei redirect che vengono ospitati da questi domini.

La soluzione più semplice è quella di sfruttare i servizi di URL shortening più diffusi; questi servizi permettono di rendere un url più breve. Questo si ottiene tramite un reindirizzamento dall'url breve a quello più lungo. Ad esempio l'url https://examplephishingsite.com/phishingpage/ può essere abbreviato in https://bit.ly/2WwFPyB. Bit.ly è un servizio creato nel 2008 dalla Bitly Inc. ed il relativo dominio bit.ly si trova tra i 10mila siti web più visitati al mondo. Viene usato quotidianamente per migliorare la lettura di un link o per semplificarne la condivisione soprattuto nei Social Network. Il suo utilizzo è usualmente lecito e pertanto il dominio se rilevato in una comunicazione fraudolenta non viene segnalato dal filtro anti-spam.

Soluzioni più avanzate prevedono la compromissione di siti web indicizzati sui motori di ricerca; una volta compromesso, un sito web viene sfruttato come redirect intermedio tra il motore di ricerca e la pagina di destinazione malevola. L'email conterrà il collegamento presente tra i risultati della ricerca effettuata sul motore di ricerca, collegamento che generalmente contiene il dominio del motore di ricerca e pertanto molto diffuso.

---

[63] https://spamassassin.apache.org/full/3.2.x/doc/Mail_SpamAssassin_Plugin_URIDNSBL.html

[64] https://www.alexa.com/topsites

Se ad esempio ricerco su Google “UniMI SSRI” ottengo come primo risultato la pagina di presentazione del corso di laurea di Sicurezza dei sistemi e delle reti informatiche. Il collegamento a tale pagina dall’elenco dei risultati è il seguente:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwjt4ILc5avoAhVNkMMKHfQiCJIQFjABegQIARAB&url=https%3A%2F%2Fssri.cdl.unimi.it%2Fit&usg=AOvVaw2Zb8JxhxC_LSd_60-pkTnx

Che effettua un redirect alla homepage del sito del corso di laurea: *https://ssri.cdl.unimi.it/it*

Ipotizzando che il sito del corso di laurea possa essere compromesso l’attaccante potrebbe reindirizzare tutti gli utenti che arrivano dal motore di ricerca ad una pagina di phishing.

Pertanto il phisher includerà nella email malevola il primo link contenente il dominio google.com che porterà l’utente ad uno o più redirect intermedi e infine alla pagina di phishing. Il dominio di Google, del precedente esempio, è ampiamente utilizzato a fini leciti e il filtro anti-spam non provvederà a identificarlo come malevolo.

9.2 Invisible characters

I filtri anti-spam effettuano un’analisi del testo della email alla ricerca di termini sfruttati abitualmente nelle comunicazioni fraudolente per richiedere alla vittima di fornire proprie informazioni personali, come “verifica subito i tuoi dati” o “conferma le tue informazioni”. Se il messaggio contiene termini ritenuti sospetti il punteggio assegnato alla comunicazione aumenta fino alla probabile attribuzione di messaggio indesiderato.

Al fine di non permettere ai filtri anti-spam l’individuazione dei termini comunemente sfruttati in una attività fraudolenta, i criminali veicolano l’email in formato HTML contenente stili grafici (CSS) in grado di nascondere alcune lettere.

Ipotizzando di voler mostrare all’utente la parola PayPal verranno introdotti caratteri invisibili all’interno di essa, tali caratteri saranno presenti nel corpo della email analizzato dal filtro anti-spam ma totalmente trasparenti all’utente che non li vedrà.

Nel codice HTML e CSS seguente la parola PayPal risulta in realtà P1a2y3P4a5l6.

```
<style>
span.hc {
  font-size:0;
}
</style>

P<span class='hc'>1</span>a<span class='hc'>2</span>y<span class='hc'>3</span>P<span class='hc'>4</span>a<span class='hc'>5</span>l<span class='hc'>6</span>
```

9.3 Ad Hoc domain

I filtri anti-spam come in precedenza menzionato effettuano verifiche sui record DNS del dominio mittente della email e sul dominio stesso per verificarne la presenza in eventuali blocklist.

Le email vengono inviate attraverso il protocollo SMTP (Simple Mail Transfer Protocol); tale protocollo sviluppato negli anni ’80 non aveva inizialmente una forma nativa di autenticazione data la scarsità di utenti in possesso di un indirizzo di posta elettronica. Da allora ad oggi si è invece reso necessario rendere più sicuro questo protocollo per verificare l’autenticità delle email in transito. Gli strumenti che garantiscono una maggiore sicurezza del protocollo SMTP sono SPF, DKIM e DMARC e la loro configurazione è consultabile mediante i rispettivi record nei DNS del dominio.

SPF (Sender Policy Framework) è un meccanismo che permette di definire i server di posta elettronica autorizzati a spedire messaggi per il dominio, consentendo pertanto a chi lo riceve di controllarne la veridicità. La lista degli host autorizzati a spedire email è pubblicata nei DNS del dominio in un record TXT creato e formattato appositamente.

DKIM (DomainKeys Identified Mai) consente al destinatario di una email di verificare la provenienza del messaggio per assicurarsi l’autenticità del mittente. Il meccanismo di basa su una o più coppie di chiavi asimmetriche; la chiave pubblica sarà presente in un record TXT del dominio creato e formattato appositamente mentre la chiave privata è conservata dal server di posta elettronica (MTA). Durante la fase di preparazione del messaggio da spedire, il server SMTP procederà a firmare digitalmente i campi “A”, “Da”, “Data” e “Oggetto” sfruttando la chiave privata. Il destinatario potrà tramite la chiave pubblica presente nei DNS del dominio mittente verificare la firma digitale apposta durante la fase di invio.

DMARC (Domain-based Message Authentication, Reporting & Conformance) è un meccanismo che si basa sulla corretta implementazione del SPF e del DKIM; combinando questi due sistemi è possibile convalidare il dominio mittente della email e l’account di posta elettronica mittente. L’abilitazione del DMARC avviane tramite un record TXT opportunamente formattato nei DNS del dominio.

Il phisher per ottenere un punteggio migliore e non vedersi contrassegnata la comunicazione come indesiderata dal filtro anti-spam può acquistare un nuovo dominio creato Ad Hoc con l’opportuna configurazione dei record SPF, DKIM e DMARC e la sicurezza di sfruttare un dominio nuovo sicuramente non presente in nessuna blocklist. Sfruttando invece gli account email gratuiti o gli spazi web compromessi non ha usualmente alcun controllo di tali record.

10. Hosting

Il web hosting è un servizio di rete che consente agli utenti di rendere accessibile il proprio sito tramite il World Wide Web (WWW). Gli Internet Service Provider (ISP) ovvero le società che offrono tale servizio dispongono direttamente o indirettamente di diversi host, alternativamente definiti “server web”, connessi ad Internet e configurati idoneamente per garantire agli utenti l’accesso al sito mediante un web browser.

La necessità dei phisher è quella di pubblicare il proprio sito web malevolo online per renderlo accessibile alle probabili vittime, e le modalità si possono suddividere in quattro differenti tipologie.

10.1 Hosting Compromesso

La crescente domanda di siti web abbinata ad una semplificazione dei processi di realizzazione e pubblicazione ne hanno notevolmente aumentato la quantità nel World Wide Web; siti web personali o di realtà societarie vengono sviluppati non solo da professionisti del settore ma anche amatorialmente sfruttando i più noti Content management system (CMS) come Wordpress, Joomla, Drupal, ecc.

La mancanza di una figura professionale nella realizzazione di un sito web comporta probabili lacune che possono riflettersi sulla sicurezza dell’intero spazio di hosting, come l’incuranza di mantenere aggiornati i software o plugin sfruttati, l’uso di password deboli o l’assegnazione errata di permessi a file e directory del file system o l’assenza di autenticazione ai database fondamentali per l’esecuzione di un CMS.

Tali lacune di sicurezza possono essere sfruttate dai criminali per compromettere lo spazio di hosting e, una volta preso il possesso, effettuarne un utilizzo malevolo come la pubblicazione di materiale di phishing o Malware.

10.2 Hosting Gratuito

Alcuni Internet Service Provider (ISP) offrono anche un servizio di hosting gratuito; tale risorsa è di facile accesso ai phisher poiché non devono ricercare siti web vulnerabili da compromettere o investire denaro per avviare la campagna malevola. Ma sussistono diversi svantaggi nell’adozione di tale soluzione.

Diversi ISP vista la crescente quantità di nuovi spazi web gratuiti richiesti per scopi illeciti, oggi giorno effettuano delle verifiche prima di offrire lo spazio di hosting, come la richiesta di un recapito telefonico che verrà successivamente convalidato mediante una chiamata o un sms,

l'invio di un documento di identità o la richiesta di una carta di credito sulla quale non verrà effettuato alcun addebito ma esclusivamente una verifica (reservation) di esistenza.

Inoltre esistono altre limitazioni che potrebbero non consentire una corretta divulgazione della campagna malevola, come:

- Limitata possibilità di scegliere il nome di dominio;
- Limitato supporto ai linguaggi web (PHP, ASP, ecc);
- Presenza di banner pubblicitari;
- Prestazioni poco performanti.

L'utilizzo di spazi web in hosting gratuito permette la diffusione di una campagna di phishing in tempi brevi e con un bassissimo costo, ma i limiti sopra descritti ed un numero sempre inferiore di ISP che offrono questo servizio, ha reso tale spazio di hosting sempre meno sfruttato dai criminali.

10.3 Hosting Dedicato

I servizi di hosting dedicato, a pagamento, offrono una più ampia offerta in base alle caratteristiche che si desidera acquistare. È possibile acquistare spazi web con il supporto a specifici linguaggi di programmazione web, con prestazioni rapportate al piano di hosting acquistato, con database SQL eventualmente configurabili, con il servizio di posta elettronica e con la possibilità di associare allo spazio di hosting un dominio creato Ad Hoc.

L'utilizzo di domini creati Ad Hoc offre al criminale la possibilità di selezionare un nome di dominio similare all'originale, sfruttando la tecnica di Typosquatting o Punycode, e di poter sfruttare il medesimo dominio opportunamente configurato anche per l'invio delle email di phishing riducendo l'efficacia dei filtri AntiSpam.

Anche per l'acquisto di hosting dedicato è necessario fornire informazioni personali e un metodo di pagamento, usualmente vengono fornite informazioni false o dati di una vittima carpiti da una precedente campagna di phishing. Analogamente, vengono sfruttate informazioni di pagamento carpite da precedenti vittime.

10.4 Fast Flux

Fast Flux[65] è una tecnica usata dalle botnet per veicolare siti di phishing attraverso molteplici host compromessi che fungono da proxy.

[65] https://www.spamhaus.org/faq/section/ISP%2520Spam%2520Issues#164

I record A delle zone DNS del dominio di phishing creato Ad Hoc vengono puntati verso una serie di IP zombi, ovvero gli host compromessi della botnet. Le zone DNS hanno inoltre valori “TTL” molto brevi, in genere meno di cinque minuti, così da garantire sempre la raggiungibilità degli IP coinvolti.

Usualmente esistono dai 5 ai 10 record A nelle zone DNS di tali domini, così da distribuire il carico e aumentare la probabilità che il sito web rimanga attivo nel caso in cui alcuni bot vengano disattivati o si blocchino.

La funzione di proxy permette di nascondere l’hosting primario sfruttato dal phisher per diffondere le pagine di phishing.

La possibilità di sfruttare molteplici host compromessi e di nascondere, mediante la funzionalità di proxy, l’hosting principale del sito malevolo garantisce al phisher un maggiore tempo di permanenza online e ne complica le operazioni di contrasto.

11. Gestione Vittime

La gestione dell'esperienza di navigazione della vittima nel sito di phishing è fondamentale; l'interazione con essa è finalizzata a raccogliere tutte le informazioni sensibili utili a completare l'attacco. Ma è altrettanto fondamentale, per l'attaccante, poter gestire e sfruttare velocemente le informazioni carpite.

11.1 Verifica Informazioni

I kit di phishing più sofisticati includono un back-end in grado di verificare in tempo reale le informazioni carpite dalla vittima. Non solo le credenziali ma anche informazioni bancarie, carte di pagamento ed eventuali indirizzi civici.

La verifica delle credenziali[66] sottratte avviene automaticamente simulando un accesso sul portale legittimo che sta subendo la campagna di phishing; qualora l'autenticazione abbia successo è inoltre possibile recuperare ulteriori dettagli sensibili da far visualizzare alla vittima. Questa tecnica permette di rassicurare ulteriormente l'utente truffato che visualizzerà alcune informazioni solamente note all'ente attaccato e non a terzi, avvalorando maggiormente la convinzione di trovarsi in un sito web legittimo.

La verifica delle carte di pagamento, abitualmente carte di credito, avviene solitamente in due fasi. La prima mediante la Formula di Luhn[67], una formula di checksum che permette di convalidare diversi numeri identificativi tra cui le carte di credito. Successivamente è possibile interrogare, tramite API, diversi servizi online che offrono la verifica del BIN (Bank Identification Number) della carta di credito e oltre a verificarne la validità possono comunicare ulteriori dettagli quali l'emettitore, il circuito e la tipologia. Informazioni utili al criminale per capire quale tipologia di utente sta frodando.

La verifica delle informazioni carpite non solo permette di mostrare alla vittima ulteriori dettagli utili ad avvalorare l'ufficialità della campagna malevola ma anche al criminale che si garantisce di acquisire solo corrette informazioni senza effettuare una successiva verifica manuale.

11.2 Salvataggio Informazioni

Le informazioni sottratte possono essere salvate, nello spazio di hosting in uso, per una più facile consultazione da parte dei criminali. Abitualmente vengono salvate in file di testo o file html, ma in caso di kit di phishing più sofisticati possono essere memorizzate in un database SQL.

---

[66] https://www.proofpoint.com/us/threat-insight/post/hook-line-sinker-sophisticated-phishing-kit

[67] https://en.wikipedia.org/wiki/Luhn_algorithm

Il salvataggio delle informazioni nello spazio di hosting in uso non é una pratica consolidata, poiché indubbiamente assicura ai criminali una più rapida consultazione ma potrebbe esporre i dati carpiti a terze parti o permettere al fornitore dello spazio di hosting di fornire ad eventuali autorità competenti tali dati per indagini sull'attività di frode.

11.3 Trasmissione Informazioni

Le informazioni raccolte possono anche essere trasmesse a servizi esterni allo spazio di hosting in uso dai criminali; questa tecnica, molto più usata rispetto al salvataggio in locale, permette anche di evitare l'esposizione dei dati a terzi.

Nella maggioranza dei kit di phishing analizzati le credenziali carpite vengono trasmesse via email direttamente al criminali, ma vengono sfruttati anche altre metodologie come l'invio sui servizi di Instant Messaging come IRC o Telegram.

L'invio ad un servizio esterno permette di raccogliere in un'unica posizione tutte le informazioni carpite rendendo più facile la consultazione e la gestione di esse quando il criminale avvia in contemporanea più campagne di phishing. L'utilizzo di piattaforme di Instant Messaging concede, inoltre, di cooperare nell'utilizzo delle informazioni raccolte qualora l'attacco sia stato eseguito da più persone.

11.4 Command and Control

Il Command and Control (C2) di una campagna di phishing é un centro di comando dal quale il criminale é in grado di visualizzare lo stato dell'attività illecita ed inviare richieste Ad Hoc all'utente adescato. I C2 nascono, in ambito informatico, agli inizi degli anni 2000, per controllare diversi dispositivi infettati da malware; tale rete é detta botnet e all'interno di questa vi sono diversi bot/dispositivi infettati e un botmaster in grado di controllare i bot tramite il Command and Control.

Nell'ambito del phishing i C2 sono arrivati negli anni successivi al 2010 a seguito dell'introduzione dell'autenticazione a due fattori, implementata in differenti soluzioni dagli istituti di credito. Questo nuovo livello di sicurezza ha reso inefficaci i tradizionali kit di phishing portando i criminali a sviluppare nuove metodiche di attacco.

Attraverso un C2 il phisher é in grado di visualizzare in tempo reale le credenziali carpite alla vittima, simularne l'accesso sul sito internet legittimo e quindi richiedere alla vittima di fornirgli il codice temporaneo o di eseguire determinate azioni (es. una chiamata ad uno specifico numero) al fine di ottenere l'accesso all'account compromesso e quindi disporre pagamenti e ottenere ulteriori informazioni sensibili. Alcuni C2 più avanzati gestiscono anche l'invio di brevi messaggi di

testo per dialogare con la vittima non solo tramite il web ma anche tramite il telefono cellulare, un canale usualmente considerato sicuro dato l'ampio utilizzo fatto dagli istituti di credito per inviare lecite comunicazioni.

12. Conclusioni

Il lavoro di tesi presentato all'interno di questo elaborato ha come obiettivo la descrizione dell'evoluzione delle campagne di phishing dagli anni '90 ad oggi, diverse nuove tecniche e vettori di attacco vengono ad oggi usati per aggirare tecniche di prevenzione o filtraggio implementate per prevenire la diffusione di questo fenomeno.

Risulta evidente come qualsiasi soluzione tecnica ad oggi implementata per contrastare il fenomeno possa essere raggirata dai criminali che sfruttano nuovi canali di comunicazioni o nuove tecniche per carpire i dati degli utenti.

È pertanto fondamentale formare gli utenti nel riconoscere una comunicazione illegittima o i meccanismi consolidati di questa tipologia di frode, affinché si possa vedere una considerevole diminuzione delle vittime.

13. Bibliografia

- *Are the Con Artists Back?A Preliminary Analysis of Modern Phone Frauds* (Federico Maggi)
- *Business Email Compromise The most costly form of phishing.* (PhishLabs)
- *Evasion Techniques: Geoblocking by IP* (PhishLabs)
- *Evasion Techniques: User-Agent Blocking* (PhishLabs)
- *Hiding in Plain Sight - Obfuscation Techniques in Phishing Attacks* (Proofpoint)
- *Hook, line, and sinker - A closer look at a sophisticated phishing kit* (Proofpoint)
- *Mafia.com. Soldi, guerra e spionaggio: inchiesta sul lato oscuro della rete* (Misha Glenny, F. M. Gimelli)
- *'Man-in-the-E-Mail' Fraud Could Victimize Area Businesses* (Ayn Dietrich-Williams)
- *On the (In)security of Google Safe Browsing* (Thomas Gerbet, Amrit Kumar, and Cèdric Lauradoux)
- *Phishing And Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft* (Markus Jakobsson)