CYBERGON
POWERED BY elmec

COME NON FARSI RUBARE UN MILIONE DI DOLLARI E VIVERE FELICI

PHISHING: AWARENESS & TECHNOLOGY

Se sei qui, significa che hai risposto giusto alla domanda all'interno della stanza di Dark Gate dedicata al *Phishing*, complimenti!

Sei ora parte della **lista VIP** per accedere a un evento nel nostro campus tecnologico, in cui ti porteremo a vivere questa iniziativa virtuale nel mondo reale.

"The human experience..."

Completa la frase raccogliendo il resto negli altri libri e conservala per ottenere un **servizio esclusivo durante l'evento: una indagine OSINT approfondita sulla tua identità digitale.**

Se vuoi ricevere informazioni aggiuntive scrivi a shockwave@cybergon.com.

Ti aspettiamo!
Team Cybergon e Elmec

Come non farsi rubare un milione di dollari e vivere felici.
Phishing: awareness & technology

INDICE

INTRODUZIONE	04
PHISHING	05
INGEGNERIA SOCIALE	06
METODOLOGIA DI ATTACCO	11
TIPOLOGIE DI ATTACCO	12
ALLEGATI E MALWARE	19
RISCHI	21
IL FURTO D'IDENTITÀ	23
PHISHING: TIMELINE	31
BEST PRACTICE	32
5 COSE	34
SECONDA PARTE	36
APPROFONDIMENTO TECNICO	37
CONCLUSIONI	53

INTRODUZIONE

Se ti capita almeno una volta al giorno di accedere alla tua posta elettronica, sei il nostro lettore ideale.

Abbiamo svolto una ricerca approfondita su un tema complesso e vasto: il phishing. L'obiettivo di queste pagine è di renderti più consapevole e pronto a riconoscere ed evitare i comuni attacchi di phishing.

Nella cybersecurity l'utente è considerato l'anello debole della catena poiché, spesso e volentieri, possiede una scarsa cultura informatica ed il primissimo filtro dietro la tastiera. Per questo motivo è fondamentale seguire un'attenta e continua formazione.

Secondo il report Clusit 2021 nel 2020 vi è stata una crescita degli attacchi rivolti all'Europa, arrivando al 25% degli attacchi totali mappati globalmente.

Parleremo di phishing, di come funziona e cosa si rischia, come utente e come organizzazione e di come proteggersi.

PHISHING
Una definizione

Il phishing è una frode informatica realizzata tramite l'invio di e-mail contraffatte per rubare informazioni personali ad un utente.

Il nome è un neologismo derivante dal termine inglese “fishing”, "pescare" e richiama quella tipologia di truffa che utilizza tecniche di ingegneria sociale sfruttando il coinvolgimento attivo della vittima.
Il phisher si finge un individuo o un ente affidabile ingannando l’utente ad eseguire un download di allegati malevoli oppure a collegarsi ad uno specifico sito web, fornendo così i propri dati come il numero della carta di credito o le proprie credenziali.

Nonostante i progressi nel settore della sicurezza informatica alcuni messaggi di posta elettronica fraudolenti riescono ancora a sfuggire ai controlli antispam poiché l’e-mail non è stata inizialmente concepita come mezzo sicuro di comunicazione.

La maggior parte delle volte, i phisher utilizzano la posta elettronica ma, sempre più spesso, le frodi avvengono tramite canali quali SMS, WhatsApp e Telegram e i social network come Linkedin, Facebook o Twitter.

INGEGNERIA SOCIALE
Le emozioni come leva

"The weakest link in any chain of security is not the technology itself, but the person operating it."

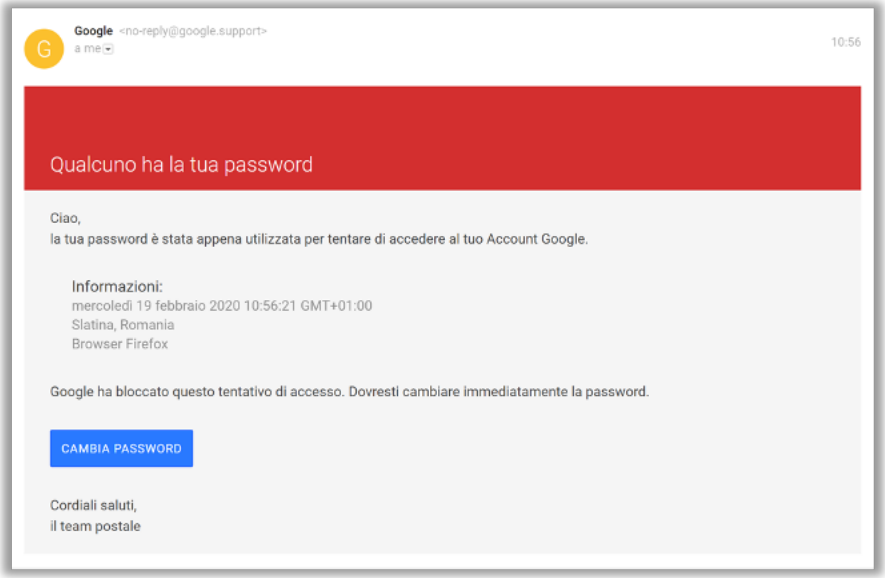
Il phisher è un criminale sempre più preparato che sa che il fattore umano è fondamentale per la riuscita del proprio attacco, così utilizza tecniche chiamate di ”ingegneria sociale” ovvero «lo studio del comportamento individuale di una persona al fine di carpire informazioni utili».

A seconda del tipo di attacco, la preparazione e lo studio della vittima e dei suoi comportamenti può essere più o meno approfondito ma, nel concreto, l’attaccante fa sempre leva su 4 emozioni umane: paura, obbedienza, gentilezza e avidità.

INGEGNERIA SOCIALE
Le emozioni come leva

PAURA

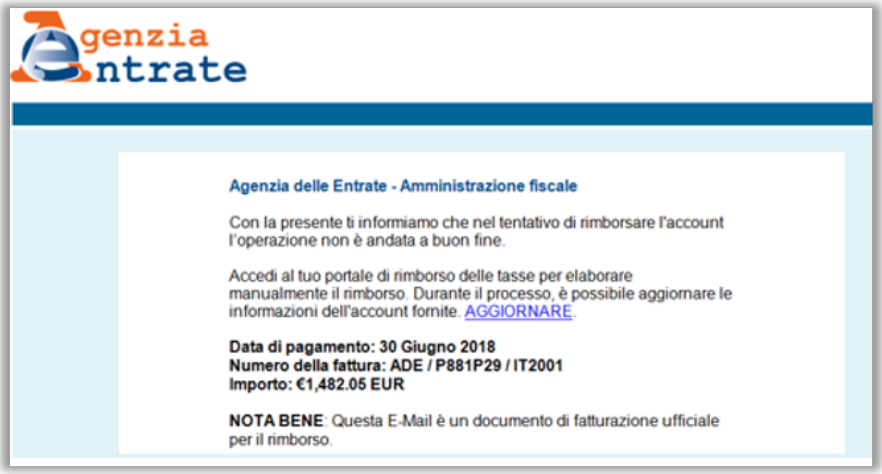
La paura è la leva preferita dei criminali: quando si prova questa particolare emozione, infatti, si è portati a reagire istintivamente senza riflettere alle azioni che si compiono.
I criminali utilizzano diversi espedienti per truffare gli utenti: una mail di phishing molto diffusa è una notifica che avvisa di furto dell'account dove l'utente viene spinto a cliccare sul cambio password. In questo modo compare un sito fasullo molto simile all'originale e, una volta inserite le credenziali, il criminale le utilizzerà per i suoi scopi illeciti.



INGEGNERIA SOCIALE
Le emozioni come leva

OBBEDIENZA

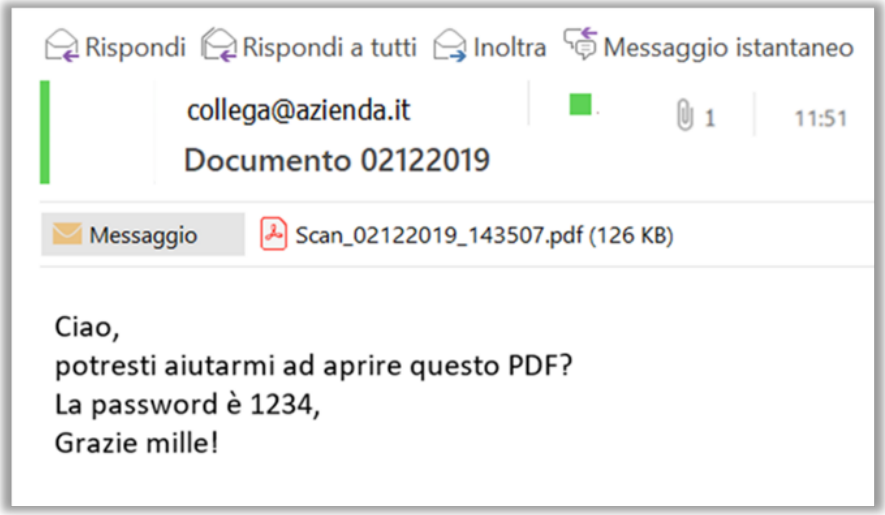
Quando si riceve un ordine o una richiesta da un'autorità come la Polizia o l'Agenzia delle Entrate, tendiamo a rispettare le istruzioni che ci vengono date senza mettere in discussione la validità della corrispondenza.



INGEGNERIA SOCIALE
Le emozioni come leva

GENTILEZZA

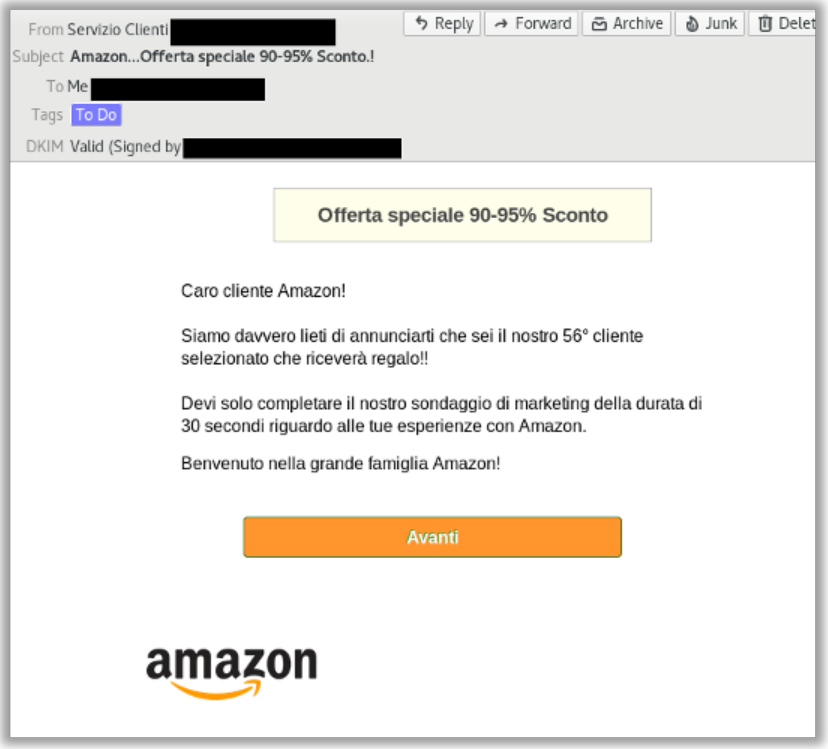
Queste campagne di phishing giocano sulla volontà di aiutare altre persone divulgando più informazioni personali di quante si dovrebbe.
Un esempio potrebbe essere la richiesta di aiuto di un collega ad aprire un allegato in PDF. Il documento in questo caso è infetto e contiene un malware (comunemente chiamato virus).



INGEGNERIA SOCIALE
Le emozioni come leva

AVIDITÀ

In questo caso, il cybercriminale offre un premio in denaro o sottoforma di sconto per attrarre l'utente.
Un esempio classico è la mail di Amazon che sembra provenire da un servizio clienti affidabile. È presente uno sconto molto interessante che spinge l'utente a cliccare ed a inserire le sue credenziali in una pagina malevola gestita dal criminale.



METODOLOGIA DI ATTACCO

Una volta comprese le abitudini e le debolezze del target individuato, il phisher può passare alla fase successiva: l'attacco. Come ogni offensiva che si rispetti, anche il phishing si basa su una strategia articolata in 5 fasi.

- **La preparazione**: il phisher prepara la mail, lavora su grafica e contenuto con un focus sui link/allegati affinché appaiano verosimili e insospettabili.

- **La lettura**: la palla passa alla vittima che legge la mail che solitamente contiene avvisi di situazioni particolari o problemi con i propri account.

- **Il click**: l'utente disattento o inconsapevole clicca sul link o scarica l'allegato che – pensa – risolverà il problema.

- **I dati**: il link che sembrava portare a un sito legittimo ha invece portato l'utente su un server controllato dal phisher. L'utente, a questo punto, inserisce i dati richiesti.

- **To be continued**: il phisher è riuscito nel suo scopo. Ora può utilizzare i dati ottenuti per fare acquisti, trasferire somme di denaro o usarli come ''ponte'' per altri attacchi.

TIPOLOGIE DI ATTACCO

Se pensiamo al phishing, ci viene in mente un'e-mail anomala il cui contenuto ci fa insospettire a causa degli evidenti errori ortografici o richieste strane e decontestualizzate.

O ancora, la mail che ci informa di aver vinto l'esclusivissimo premio «solo per oggi!».

E' così in alcuni casi, ma non si esaurisce qui: il phishing continua a evolvere e ad oggi possiamo contare 4 diverse tipologie di attacco con differenti sfumature e caratteristiche che sono:

- COMMON PHISH
- SPEAR PHISHING
- CLONE PHISHING
- WHALING SHARK

TIPOLOGIE DI ATTACCO
Indicatori comuni

Con il passare del tempo e l'introduzione di nuove tecnologie, il phishing ha subito delle evoluzioni, ma esistono degli "indicatori" comuni a tutte le tipologie di attacco che possiamo considerare per non cadere nella trappola, sia per gli account di posta privati che aziendali.

- **Saluti generici:** le aziende si rivolgono ai loro clienti chiamandoli per nome e cognome. Quando un messaggio comincia con “Gentile Signore/a” o «Gentile Cliente» bisogna insospettirsi.

- **Too good/bad to be true:** se la notizia è esagerata (vincite o bollette astronomiche, ricompense o conseguenze severe) probabilmente non è vera.

- **Link**: spesso i link sono camuffati in domini verosimili a quelli noti e comuni. In realtà nascondono sottodomini diversi. Verifica, passandoci sopra il mouse, che l’URL corrisponda al link presente nella mail e che ci sia il protocollo https (ma non sempre è garanzia di affidabilità).

- **Allegati:** ogni allegato potrebbe essere potenzialmente malevolo anche se ritenuto sicuro dall’antivirus e dell’antispam; nel dubbio non aprirlo.

- **Mittente:** il phisher riesce facilmente ad attuare la sua truffa perché molti servizi di posta elettronica hanno deciso di omettere l’indirizzo mail e far visualizzare solo il nome e cognome.

- **Urgenza:** il phisher fa leva sulla disattenzione e sulla fretta della vittima, dando carattere d’urgenza alla mail.

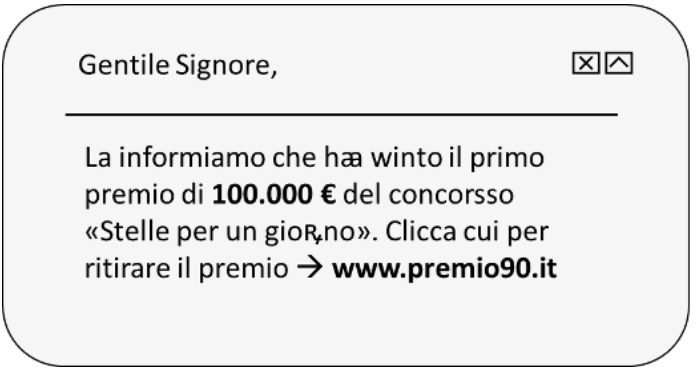
TIPOLOGIE DI ATTACCO

Common phish

È la tipologia più vecchia di phishing che trova origine nelle "catene di Sant'Antonio" o nelle fake news. L'obiettivo è sempre uno: il denaro.

La vittima è scelta casualmente, l'invio è massivo a milioni di indirizzi e la sua riuscita deriva dalla non familiarità con il mondo informatico. Infatti, molto spesso, le vittime sono persone più anziane e inesperte.

Il phisher, in questo caso, non si affida tanto alla propria preparazione, anzi, le mail risultano generiche e grossolane, quanto alla probabilità che almeno l'1% dei riceventi della mail clicchi senza controllare. In questo tipo di attacco è molto comune trovare errori di ortografia e grammatica, in particolare in Italia.
Il testo, probabilmente, è stata scritto in un'altra lingua da paesi come Cina, Russia, Iran e India che fanno largo uso del traduttore automatico. Attenzione anche a lettere di altri alfabeti o parole non accentate.

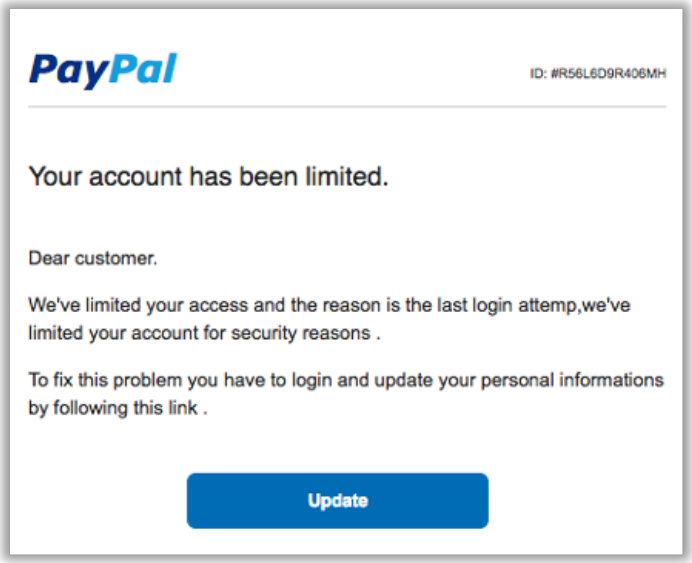


TIPOLOGIE DI ATTACCO

Spear phishing

Gli indicatori per riconoscere la frode sono gli stessi di cui abbiamo già parlato. In questo caso però l'attaccante **impersonifica sempre un'azienda**.
Questo è il tipo di attacco più diffuso con il 91% di propagazione. Le combinazioni tra social media e informazioni trovate su Google possono essere usate per personalizzare i contenuti.

Esiste una classifica delle aziende maggiormente impersonificate con lo spear phishing. Sul podio troviamo PayPal, Facebook e Microsoft, seguite da altri grandi player quali Netflix, WhatsApp e Amazon.

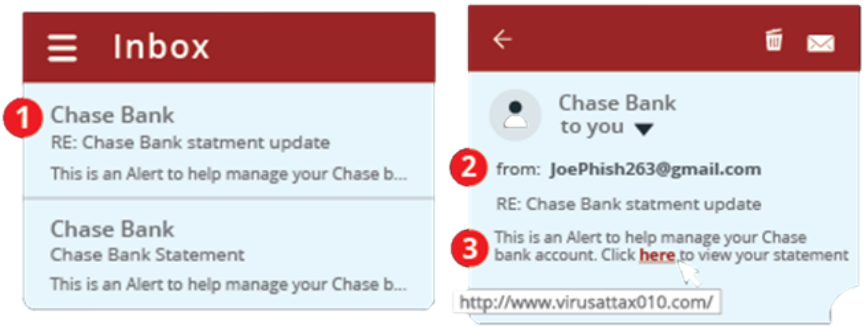


TIPOLOGIE DI ATTACCO

Clone phishing

Questo tipo di mail si presenta come una risposta ad una mail (R: oppure RE:) inviata precedentemente ad un destinatario. Si riceve una copia pressoché identica di una mail che si aveva già inviato con una modifica: sono stati aggiunti link o allegati diversi da quelli originali, ovviamente malevoli, e la mail proviene da un indirizzo mittente contraffatto.

L'attaccante sfrutta la fiducia dell'utente che, riconoscendo la risposta ad una mail già inviata, abbassa la propria soglia di attenzione e non si pone interrogativi.
Osservando il display name della mail, nel nostro caso "La banca", si può riscontrare una differenza tra il nome che compare e l'indirizzo di posta e-mail che ha effettivamente risposto (JoePhish263@gmail.com).
Dal punto di vista tecnico si può infine analizzare l'header della mail che può essere paragonato alla tracciabilità di un prodotto alimentare: ti mostra il server da cui è passata la mail e il ''giro'' che ha fatto.



TIPOLOGIE DI ATTACCO

Whaling shark

Whaling Shark significa in inglese "caccia allo squalo balena". Un nome affascinante per un tipo di attacco altrettanto pericoloso.

Il target di questa tipologia di phishing è esclusivamente la figura manageriale: CEO, CIO, CFO.
Il contenuto è creato su misura per il target e si presenta come un problema amministrativo o una lamentela di un cliente, spesso con un oggetto cosiddetto "clickbait", che spinge subito ad aprire la mail.
È comune trovare parole come «urgente», «fallimento», «causa» o «pagamento».

I whaleshark, ovvero i manager all'interno di un'azienda, sono spesso occupati e distratti dal loro lavoro e vengono facilmente ingannati nella routine dell'ufficio.

TIPOLOGIE DI ATTACCO

Whaling shark: una variante

Esiste una variante che si chiama **Business Email Compromise** (**BEC**) o **CEO Fraud.** L'attaccante in questo caso si presenta come un amministratore delegato e utilizza la propria autorità per richiedere un pagamento urgente e cospicuo. Spesso viene richiesta massima riservatezza per la transazione. La vera differenza con lo spear phishing è che, in questa particolare tipologia, viene impersonificata, non più un'azienda, ma una figura apicale.

Il consiglio in questo caso è quello di ''disturbare'' il diretto interessato per assicurarsi della veridicità della richiesta. Come dicono gli inglesi «*better safe than sorry*».

ALLEGATI E MALWARE

Abbiamo fino ad ora parlato di link malevoli e accennato al fatto che le mail di phishing possono anche sfruttare allegati per veicolare un'infezione e recuperare i dati che interessano l'attaccante. Come?
Attraverso i malware.

Un malware è un particolare tipo di software creato per compiere operazioni non volute e dannose sul PC di una vittima. L'obiettivo dell'attaccante è quello di installarlo in modo permanente e difficilmente individuabile.

È bene ricordare che ogni allegato potrebbe essere potenzialmente malevolo anche se ritenuto sicuro dall'antivirus e dell'antispam. Si può dedurre quindi l'importanza di riconoscere l'estensione del file in quanto quest'ultima può fornire importanti indicazioni sulla potenziale pericolosità dell'allegato. Nel dubbio rimane sempre valido il consiglio di non aprire l'allegato per non far eseguire programmi malevoli.

Esistono vari tipi di malware: virus, trojan, ransomware, rootkit... Il phishing è uno dei metodi principali per la loro diffusione insieme alle chiavette USB.

ALLEGATI E MALWARE
Best practice

Il Malware Spam o Malspam è il termine che si riferisce al malware che viene veicolato in allegato ai messaggi di posta elettronica.

Le best practice da seguire per evitare di rimanere infettati sono:

- Mai scaricare o visualizzare allegati di e-mail da mittenti sconosciuti;

- Non eseguire mai file sconosciuti, non aprire file zip e far attenzione anche ai PDF; questi tipi di file possono eseguire Flash/Javascript o addirittura lanciare applicazioni esterne;

- Non abilitare le macro di Office in caso di dubbio;

- Spesso i file hanno doppia estensione, come "nomefile.jpg.exe"; Windows mostrerà il file come "nomefile.jpg" nascondendo il fatto che in realtà è un eseguibile; per ovviare a questo, disabilitare nelle opzioni di "Esplora Risorse" la voce “nascondi estensioni per tipi di file noti”.

RISCHI
Obiettivi del phisher

SunTzu ne ''l'Arte della guerra'' diceva: «conosci il tuo nemico».

Il guadagno per queste attività, in proporzione al rischio, è assolutamente conveniente. È evidente che l'obiettivo primario del nostro antagonista è il denaro.
Ma questo non è per noi utenti l'unico rischio.

- **Perdita di denaro**: il denaro è l'incentivo principale del phisher.

- **Furto d'identità:** l'identità digitale è l'insieme degli attributi di una persona che la caratterizza in modo univoco nel mondo virtuale; quando un utente deve identificarsi per compiere determinate operazioni lo dimostra tramite una procedura di autenticazione. La procedura di autenticazione è tanto più solida quanti più fattori vengono controllati.

- **Partecipazione ad attività illegali:** ovviamente la vittima è inconsapevole. L'attaccante sfrutta la macchina del suo target per infettare altri sistemi. Il computer diventa così parte di una botnet: una rete di pc infettati, controllati dal botmaster, il nostro criminale.

RISCHI
Obiettivi del phisher

- **Sfruttamento di risorse della vittima**: avviene installando software – come, ad esempio, un Trojan BitCoinMiner – per sfruttare la CPU e generare cryptovaluta; questo causa rallentamenti nell'esecuzione dei programmi e un surriscaldamento della batteria.

- **Inserimento della mail della vittima in una lista di spam:** molte delle e-mail che riceviamo oggi non sono semplicemente testuali ma sono a tutti gli effetti delle pagine web contenenti immagini. Per vederle l'utente deve scaricarle dal sito web dove risiedono e in questo modo la vittima fa sapere all'attaccante, proprietario della pagina malevola, che la casella di posta è "attiva" ed effettivamente utilizzata. A questo punto, l'attaccante la inserirà in una lista di spam e la vittima inizierà a ricevere e-mail non volute che potrebbero essere anche il veicolo per un'altra tipologia di attacco informatico.

- **Rivendita dei dati personali o sanitari:** la tipologia di informazioni che vale di più sono i dati sanitari e biometrici venduti fino a 500 dollari nel Darkweb. Un'altra pratica molto comune è vendere informazioni personali ad aziende per profilarvi oppure venderle ad altri criminali per confezionare attacchi più mirati.

IL FURTO D'IDENTITÀ

Riteniamo che sia necessario dedicare un piccolo approfondimento al tema del furto di identità che, come abbiamo detto, è uno degli obiettivi primari dei phisher e uno dei rischi più impattanti per gli utenti.

Si verifica quando un criminale informatico **si impadronisce delle credenziali di un utente** per utilizzarle poi per uno scopo illecito.

Il motivo per il quale il tema è diventato così importante negli ultimi anni è che spesso le aziende trattano, durante la loro routine lavorativa, i dati dei propri dipendenti e clienti: ad esempio il numero di telefono o l'indirizzo e-mail.

Il furto di identità gira intorno a 3 elementi chiave: l'indirizzo e-mail (personale o aziendale), username e password.

Prima di analizzare questi tre elementi è utile comprendere la pericolosità dell'essere ''impersonificati'' in rete e in particolare imparare quali possono essere **semplici regole di buon senso** da seguire.

IL FURTO D'IDENTITÀ

Come avviene

Come può nel concreto avvenire questo particolare tipo di furto?

Facciamo un esempio pratico: quando deleghiamo una persona per prendere un pacco a nostro nome, ci viene richiesto di fornirgli la copia di un nostro documento di identità e la nostra firma.
In rete invece è un po' diverso: non c'è più una persona fisica, ma ci si identifica solamente tramite le informazioni che si possiedono.
Queste sono spesso molto facili da reperire per un criminale informatico e ancor più facili da utilizzare una volta ottenute.

Per il semplice fatto che la rete è un luogo immateriale, potremmo avere più identità associate a una singola persona oppure impossessarci di un'identità autentica per compiere atti illeciti, basti pensare che chiunque può creare un account mail con il nostro nome e cognome (tranne nel caso della PEC, che richiede un documento di identità per la registrazione)

Da qui nasce il dilemma: come possiamo collegare qualcosa di fisico, la nostra persona, a qualcosa di immateriale, un account su un provider di posta elettronica?
La regola che vale nel mondo della Cybersecurity è che chi possiede la password dell'account, generalmente, controlla anche quella specifica identità.
La casella di mail è sempre collegata ad altri account e quindi, in caso di furto, diventa critico potersi riappropriare della propria identità e riottenerne il controllo completo.

IL FURTO D'IDENTITÀ
Conseguenze e consigli

Immaginiamo che un criminale riesca a impossessarsi della copia della nostra carta d'identità: può tenerla per sé e utilizzarla oppure rivenderla nel dark web, il mercato nero della rete.
Questo è un tema particolarmente critico, perché chi ha in mano questo tipo di dati, possiede di fatto un'identità. Identità che spesso vengono utilizzate per riciclare il denaro sporco dai cybercriminali stessi che utilizzano i dati in loro possesso per registrare conti correnti a nome della vittima.

Questa pratica è conosciuta anche con il nome di ''Money Mule'', letteralmente "mulo da soldi" e ha come obiettivo il riciclaggio di denaro derivante da attività illecite, in particolar modo dalle campagne di phishing.

Le vittime spesso non sono consapevoli dell'illegalità di queste pratiche o vengono adescati con dei falsi contratti di lavoro pensando semplicemente di svolgere un'attività finanziaria del tutto regolare. In realtà commettono un reato grave e favoriscono attività criminose come il traffico di droga e frodi online.
Per tutelarsi, consigliamo di seguire qualche semplice regola di buon senso:

- Non mettere mai a disposizione di terzi il tuo conto bancario;
- Comunica i tuoi dati bancari e personali soltanto a persone che conosci e di cui ti fidi;
- Segnala subito alla polizia postale le offerte che prevedono una ricezione di fondi sul tuo conto corrente.

IL FURTO D'IDENTITÀ
Mail aziendale

Naturalmente siamo a rischio come nella nostra vita privata, così in quella lavorativa. E anche gli strumenti aziendali devono essere utilizzati consapevolmente.

Gli attacchi chiamati ''credentialstuffing'', letteralmente "riempimento di credenziali", sfruttano il fatto che le persone utilizzano le stesse credenziali per accedere a più servizi come applicazioni e siti, porgendo generalmente poca attenzione per la sicurezza dei propri profili. Questo è altrettanto rilevante se si parla di credenziali per utenze aziendali.
Ma dove prendono i phisher il nostro indirizzo?

Bisognerebbe evitare registrazioni o iscrizioni a siti web con la mail aziendale, perché spesso – soprattutto quelli meno affidabili – permettono la divulgazione del nostro indirizzo mail a società terze o a phisher che li utilizzano per inviare mail contraffatte con allegati malevoli. I virus non solo intaccheranno così il computer sul quale vengono scaricati, ma anche tutti i restanti computer collegati alla rete del vostro ufficio con il rischio di creare un grave danno per l'azienda dove lavorate.

Ricorda che i phisher cercano continuamente potenziali liste di destinatari analizzando forum online o siti che inviano newsletter, rubando liste di mail da altri siti che possono avere un livello di sicurezza più basso come, ad esempio, il negozio sotto casa al quale ci siamo iscritti per ricevere scontistiche.

IL FURTO D'IDENTITÀ
utilizzo della mail

Come gestire le nostre caselle di posta.
Come abbiamo detto, l'account aziendale va utilizzato per scopi puramente lavorativi, e quello privato?

Quello che consigliamo in questo caso è di avere un indirizzo di posta in cui utilizzeremo un nickname (ovvero un nome di fantasia che vi rappresenti oppure un soprannome non riconducibile a voi) e una casella di Posta Elettronica Certificata, PEC, che ha un costo annuo irrisorio ed è registrabile solo con un documento d'identità.

Perché è importante differenziarle.
Possiamo utilizzare l'email con il nickname per quei siti poco affidabili e per le newsletter che ci arrivano settimanalmente, mentre per i documenti importanti come quelli amministrativi e per il nostro conto in banca useremo la PEC.

Se dovessimo un giorno ricevere qualcosa di davvero importante sull'email ''del tempo libero'', sapremo che potrebbe trattarsi di phishing non gestendo queste pratiche se non attraverso l'altra casella di posta.

IL FURTO D'IDENTITÀ

Password a prova di criminale

La sicurezza dei nostri account, siano essi privati o aziendali, passa anche dalle password.
Come possiamo creare una password che sia a prova di criminale informatico?

Tecnicamente non esistono password che un cracker, ovvero coloro che forzano gli accessi degli account, non possa bypassare.

Quello che dovremmo fare è non facilitargli il compito optando per una password troppo semplice e banale da indovinare. Spesso, come avrai notato, nella creazione di una nuova password, viene richiesto un minimo di requisiti: numero dei caratteri, maiuscole, numeri e caratteri speciali.

Una password ''complessa'' è più sicura.

Curiosità: il tempo per craccare una password di 12 caratteri alfanumerici casuali è di 600 anni.

IL FURTO D'IDENTITÀ

Password a prova di criminale

Vediamo una serie di requisiti utili a creare password efficaci.

- Non deve essere banale (come il proprio nome, data di nascita, nome dei figli, ecc.) né di senso compiuto: evitare parole facilmente trovabili sul dizionario;
- Deve esserci una lunghezza minima, in quanto si distingue anche per la quantità di caratteri che la compone: buona regola sarebbe di usarne almeno 12.
- Una sequenza in cui si utilizzano caratteri speciali e cifre permette di alzare la casualità della password e aumentare il tempo necessario al criminale informatico per decifrarla ed entrare nel vostro account.
- Non serve sostituire le lettere con i numeri perchè, nell'ambito informatico, è un linguaggio molto comune: L3GG3R3 3 5CR1V3R3 NUM3R1 4L P0570 D1 L3773R3 3' UN PR0C3550 P1U770570 53MPL1C3.
- Non usare una sequenza sulla tastiera come «qwerty» o di numeri come «123456». Sono tra le primissime ad essere indovinate.
- Utilizzare una passphrase cioè una frase di senso compiuto: è sicura e si può ricordare senza doverla appuntare per iscritto. La principale differenza fra "passphrase" e "password" è il numero di caratteri utilizzato: 20/30 nel primo caso e 8/10 nel secondo.
- Non trascrivere su un foglio le password ma utilizzare un ''password manager'': un tool di cui serve ricordare la password di accesso (la cosiddetta masterpassword) per accedere a tutte le password salvate.

IL FURTO D'IDENTITÀ

Password: perché differenziarle

Uno degli errori più comuni che si commettono nella gestione delle proprie password è di utilizzare sempre la stessa in servizi web diversi.

Il solo fatto di doversi ricordare a mente tante password, magari anche complesse, sicuramente non invoglia l'utente a seguire le best practice.
Si stima però che metà delle persone online utilizzi dalle 2 alle 4 password: queste magari possiedono tutti i requisiti di sicurezza ma vengono purtroppo usate per un elevato numeri di siti.

Perché dobbiamo differenziarle:
La motivazione è che non possiamo evitare che i servizi web a cui ci iscriviamo rimangano inviolati. Un caso molto noto nel mondo della Cybersecurity è LinkedIn: nel 2012 infatti sono state pubblicate online circa 170 milioni di credenziali.

I criminali informatici cercano di forzare i database dei siti e dei social network ai quali ci iscriviamo. Se viene utilizzata un'unica password per diversi account, non potremo impedire che, in caso di breccia in uno di questi siti, tutti gli altri account con quella stessa password vengano violati.
È comune tra gli utenti aggiungere o cambiare una piccola parte della password per poter differenziarle, per esempio: "phishing01" viene trasformata in "phishing02".
Questa sequenza di numeri la rende di fatto una password molto debole perché, con alcune tecniche avanzate, è possibile per i cyber criminali riuscire nella violazione.

PHISHING
Timeline

1987 — Viene descritta la prima tecnica di phishing

1996 — Il termine phishing appare in «The Hacker Quarterly»

2004 — Il phishing è parte affermata dell'economia del crimine

2009 — Trasferiti $1,9 milioni attraverso conti bancari di Experi-Metal

2011 — Campagna di phishing contro alti ufficiali dell'esercito

2013 — Il Ransomware Cryptolocker infetta 250.000 PC

2018 — Campagne di phishing con obiettivo Cryptovalute

2019 — +24% di attacchi durante BlackFriday

BEST PRACTICE
Minimizzare il rischio

Come si fa a non cadere vittima di tutto questo?
Partiamo dal presupposto che non è possibile eliminare del tutto le mail di phishing o lo spam.
Tuttavia possiamo adottare comportamenti preventivi.

- **Password**: usa password efficaci come la passphrase, cambiale spesso e diversifica a seconda dell'account (social; online banking; e-mail...).

- **Newsletter:** iscriviti solo a quelle che ti interessano. Spesso l'inganno si nasconde dietro il tasto ''unsubscribe'' di quelle a cui, in realtà, non ti sei mai iscritto.

- **E-mail:** è raccomandabile avere più indirizzi e-mail e ''usa e getta'' creati ad hoc per i siti di dubbia affidabilità. Usa la PEC per i servizi amministrativi e finanziari.

- **Spam:** i gestori di posta elettronica hanno, solitamente, sistemi di gestione dello spam. Controlla che siano attivi.

- **Pagamenti:** quando fai acquisti online utilizza carte prepagate, così da non condividere dati del conto bancario, che potrebbero essere sfruttati dal phisher.

BEST PRACTICE
Gestire le conseguenze

Se, in qualità di utente, le precauzioni prese non sono state sufficienti o l'attaccante ci ha colpiti in un momento di disattenzione o ancora ha effettuato un attacco particolarmente ben studiato ed efficace (in fondo, capita), ecco qualche consiglio:

- **Contatta la tua banca:** informa il tuo istituto bancario che hai potenzialmente fornito credenziali sensibili.
- **Modifica le password:** cambia le password e tieni monitorate le attività sui tuoi account.
- **Antivirus:** aggiornalo (se non l'hai ancora fatto!) ed effettua una scansione sui tuoi device.
- **Informa la società impersonificata:** se il phisher ti ha tratto in inganno spacciandosi per un'organizzazione (abbiamo già parlato delle più comuni), informa la loro assistenza clienti.

CINQUE COSE DA NON FARE

1. Non fare clic su link nelle mail che ti chiedono di inserire informazioni riservate. È meglio andare direttamente alla fonte scrivendo voi stessi l'indirizzo

2. Non condividere eccessivamente sui social media. Questi dettagli possono fornire ai criminali la tua posizione, le munizioni per creare attacchi di spear phishing e le risposte alle domande di sicurezza. Pensa prima di condividere!

3. Non scaricare nessun allegato se non lo stavi aspettando! Aprilo solamente se sei sicuro di quello che vi è dentro.

4. Non riutilizzare mai le stesse password per diversi siti Web o servizi.

5. Non rispondere mai alle domande di recupero dell'autenticazione (ad es. Qual è il nome da nubile di tua madre?) con risposte reali. Sfortunatamente, ciò significa che dovrai scrivere una risposta diversa per ogni sito Web che li richiede, ma avrai molte meno probabilità di avere il tuo account rubato.

CINQUE COSE DA FARE

1. Sii sempre scettico su qualsiasi fattura imprevista o richiedi di ottenere o pagare qualsiasi cosa utilizzando carte prepagate.

2. Sapere a chi segnalare eventuali e-mail sospette sul posto di lavoro. Non eliminare l'email, segnalala. Condivisione è conoscenza.

3. Fare attenzione ai messaggi SMS sospetti. La tua banca non ti chiederà MAI di accedere al tuo account da un SMS.

4. Investire in uno strumento di gestione delle password: nessuno ha il tempo di ricordare tutte quelle password!

5. Confermare la validità della richiesta di cambio IBAN attraverso un controllo incrociato, anche se a farla è il tuo capo. Meglio prevenire che curare.

SECONDA PARTE

Speriamo fino ad ora di aver incontrato le tue aspettative, caro lettore, rispondendo a domande quali:
cos'è il phishing; su cosa fa leva il criminale (o l'organizzazione criminale) che si cela dietro gli attacchi e come agisce; come faccio a riconoscere le tante tipologie di phishing utilizzate; cosa posso fare per prevenire gli attacchi.

Una serie di risposte che ben si sposano con i dubbi che quotidianamente ci poniamo in qualità di utenti.

È lecito, per chi lavora e svolge ruoli di responsabilità in azienda, chiedersi come cambino le cose quando ad essere coinvolte sono proprio le imprese, in particolare, le piccole e medie, che in Italia rappresentano il 92% delle attività.

Nell'introduzione abbiamo detto che un'efficace strategia di difesa passa attraverso la fondamentale consapevolezza dei singoli, ma questo non basta.

APPROFONDIMENTO TECNICO

Introduzione

Vediamo nelle prossime pagine quali sono i passi da fare in ottica di costruzione di una strategia di difesa della propria azienda.

Insieme vedremo diverse funzionalità di ispezione e analisi dei contenuti delle mail.
In particolare, vedremo quattro passaggi fondamentali come:

- **Verifica dell'identità:** Crittrografiaantispoofing, Standard di identificazione del mittente, Reputation e Signatures.
- **Difesa dagli URL malevoli**: Protezione dagli URL, E-mail Gateway, Filtri Bayesiani.
- **Mitigazione degli allegati malevoli:** Analisi Euristica, Sandbox, Data Loss Prevention.
- **Formazione degli utenti:** Phishing test e corsi di awareness.

APPROFONDIMENTO TECNICO
Verifica dell'identità

CRITTOGRAFIA ANTISPOOFING: Le mail non possiedono intrinsecamente la crittografia end-to-end e per evitare lo spoofing, ovvero l'impersonificazione del mittente, è necessario implementare questa funzionalità aggiuntiva.

Sono due le tipologie più utilizzate:
Il Secure/Multipurpose Internet Mail Extensions (S/MIME) e l'Open PGP (Pretty Good Privacy).

S/MIME
È uno standard per la crittografia a chiave pubblica e la firma digitale di messaggi di posta elettronica in formato MIME, che permette di inserire in un qualsiasi messaggio di posta, oltre al semplice testo, contenuti multimediali quali immagini, video e audio.

OPEN PGP
È probabilmente il metodo a crittografia asimmetrica più adottato al mondo in cui il destinatario del messaggio ha generato precedentemente una coppia di chiavi collegate fra loro, una chiave pubblica ed una privata. La chiave pubblica del destinatario serve al mittente per cifrare una chiave di sessione per un algoritmo di crittografia simmetrica; questa chiave viene quindi usata per cifrare il testo in chiaro del messaggio.

APPROFONDIMENTO TECNICO

Verifica dell'identità

S/MIME offre gli stessi servizi di PGP, ma adotta formati diversi ed incompatibili. Diversamente da PGP, che usa un sistema web of trust per la distribuzione delle chiavi pubbliche, i corrispondenti che usano S/MIME necessitano l'acquisto di una Certification Authority, che compie diverse operazioni di autenticazione e validazione del richiedente fino al rilascio di un certificato digitale.

Due caratteristiche fondamentali di S/MIME sono la firma digitale e la "busta digitale" (digital envelope): la chiave simmetrica utilizzata per crittografare il messaggio viene cifrata con la chiave pubblica del destinatario e inviata assieme al messaggio stesso. Oltre a garantire l'integrità e la riservatezza del messaggio, S/MIME prevede l'autenticazione del proprietario di una chiave pubblica.

L'uso appropriato di questi due sistemi rende praticamente impossibile che un intermediario fra mittente e destinatario possa giungere al messaggio d'origine, ad esempio tramite l'attacco man in the middle. Occorre quindi che gli utilizzatori dei crittosistemi non diventino loro stessi la via per violare i loro dati.

APPROFONDIMENTO TECNICO
Verifica dell'identità

Sono tre gli Standard piùutilizzati per l'identificazione del mittente:

DMARC
Domain-based Message Authentication, Reporting & Conformance: complesso sistema di validazione dei messaggi. Permette al server del mittente di definire le regole con cui trattare i messaggi non validati (messa in quarantena, spam, eliminazione)

SPF
Sender Policy Framework: consente di verificare che una e-mail inviata da un dato dominio arrivi effettivamente da uno degli host abilitati dai gestori del dominio stesso. Questo elenco viene reso pubblico attraverso un record DNS.

DKIM
Domain Keys Identified Mail: è un metodo di autenticazione delle e-mail, realizzato per prevenire lo spoofing. Consente di verificare la provenienza del messaggio in modo da accertarsi dell'autenticità del mittente, mediante l'apposizione di una firma digitale.

APPROFONDIMENTO TECNICO
Verifica dell'identità

Combinando opportunamente SPF e DKIM diventa possibile validare il mittente di una e-mail, garantire cioè che il messaggio provenga realmente dal dominio e dall'utente specifico. Per simmetria la mancata validazione può consentire un'immediata individuazione di messaggi di spam, di phishing o in cui comunque il mittente reale sia stato mascherato. Affinché la validazione tramite DMARC sia efficace è necessario che questo protocollo sia implementato sia sul server del destinatario che sul server del mittente.

Per comprendere il funzionamento di DMARC poniamoci in una condizione semplificata in cui l'indirizzo mitt@esempio.com invii una email all'indirizzo dest@esempio.org. Durante l'invio il server example.com aggiunge al messaggio l'intestazione (header) DKIM generata con un sistema di crittografia a doppia chiave. Quando l'e-mail arriva sul server example.org il protocollo DMARC consente di effettuare una serie di controlli di validità prima che il messaggio venga scaricato dal destinatario. Utilizzando la chiave pubblica DKIM di example.com il server example.org procede, anzitutto verificando che il messaggio arrivi effettivamente dall'indirizzo dichiarato e che non sia stato alterato durante il suo percorso, successivamente, attraverso SPF, il server verifica che l'host da cui è partito il messaggio sia tra quelli abilitati. Solo se entrambi i controlli vengono superati il messaggio è reso disponibile nella casella del destinatario. Quando invece uno o entrambi i controlli non vengono superati possono scattare diverse misure di protezione.

APPROFONDIMENTO TECNICO
Verifica dell'identità

I controlli per il perimetro aziendale dipendono dalle signatures e dalla reputation che intraprendono azioni per cogliere gli attacchi nei punti di entrata della rete:

- WHITELIST AND BLACKLIST: un elenco di indirizzi o domini di provenienza dai quali accettare o rifiutare i messaggi di posta elettronica senza applicare il filtro antispam. I trigger, cioè gli attivatori, possono essere parole, frasi o anche formattazioni particolari che caratterizzano lo spam. Quando un'e-mail raggiunge un determinato "punteggio" viene automaticamente inoltrata nella cartella relativa ed entra in blacklist.

- DOMAIN CHECK: una lista di IP di server noti per l'invio di spam o di provider di posta elettronica. I provider che utilizzano queste blacklist bloccano tutte le email inviate da questi IP.

- IP REPUTATION: vene creato un elenco di indirizzi IP considerati affidabili e qualsiasi traffico e-mail proveniente da un indirizzo IP sarà esonerato dal controllo DNS Blackhole list. La reputazione dipende dai vari punteggi associati all'identificazione del mittente, che si determina in funzione di un indirizzo IP d'invio e del nome di dominio utilizzato e in base alla qualità delle campagne e-mail, alla frequenza, all'entità e all'interazione con l'utente. Se è superiore al livello di policy impostato la mail viene bloccata.

APPROFONDIMENTO TECNICO

Verifica dell'identità

- SPAM SIGNATURES: questo metodo compara le e-mail in entrata con le signatures dei database di spam conosciute. Il vantaggio è di avere falsi positivi molto ridotti in quanto viene effettuato un controllo incrociato. Il rovescio della medaglia è che deve esistere un database spam non zero-day costantemente aggiornato con le diverse signatures.

- CONTROLLO SUL CHEKSUM: Il checksum è una sequenza di bit che, associata al pacchetto trasmesso, viene utilizzata per verificare l'integrità di un dato o di un messaggio che può subire alterazioni durante la trasmissione sul canale di comunicazione.

APPROFONDIMENTO TECNICO
Protezione dagli URL malevoli

Nonostante già molti browser abbiano implementato plug-in per bloccare l'utilizzo sospetto di Javascript nelle pagine web, diventa fondamentale dotarsi di un servizio che rivela gli URL dannosi nelle mail sospette.

Questa funzionalità dell'antispam riscrive i link malevoli selezionati in modo tale che i client vengano reindirizzati attraverso un ulteriore filtro. Ciò impedisce che gli URL precedentemente sconosciuti o attendibili vengano armati dopo il recapito nella posta in arrivo.

La *Vulnerabilità Open Redirect* consente ad un attaccante di manipolare un URL al fine di dirottare un utente su un sito malevolo sfruttando un URL lecito. La vittima potrebbe cliccare sul sito A per poi finire reindirizzato sul sito B senza accorgersi di alcun cambiamento, soprattutto se l'attaccante ha creato una versione credibile del sito di destinazione.

L'e-mail gateway della posta in entrata è un server attraverso il quale transita tutta la posta inviata al dominio. La corretta configurazione assicura che si determini correttamente l'IP di origine del messaggio per eseguire un controllo SPF ed evitare di classificare un messaggio legittimo come spam.

APPROFONDIMENTO TECNICO

Protezione dagli URL malevoli

Generalmente, prima di recapitare la posta, il gateway la elabora archiviandola o filtrandola, per poi trasmettere le e-mail al server di posta che le consegna ai destinatari.
Il servizio di posta non esegue il controllo dei record SPF sugli indirizzi IP inclusi nell'elenco IP del gateway mentre per il controllo DMARC, che deve essere eseguito dal gateway in entrata, verrà ignorato per i messaggi provenienti dagli host elencati.

In via facoltativa bisognerebbe:

- Configurare il rilevamento automatico di IP esterni.
- Rifiutare la posta non inviata dal gateway.
- Richiedere che le connessioni dal gateway utilizzino il protocollo TLS (Transport Layer Security).
- Configurare la gestione dello spam in base ai tag dei messaggi del gateway.

APPROFONDIMENTO TECNICO
Protezione dagli URL malevoli

Il filtro bayesiano applica all'analisi delle e-mail un teorema secondo il quale ogni evento a cui è attribuita una probabilità è valutabile in base all'analisi degli eventi già verificatesi.
Gran parte dei software antispam adotta questa tecnica complementare: è una forma di filtraggio che si basa sull'analisi del contenuto delle e-mail e prende il nome dal noto matematico Bayes.

Nel caso dell'analisi antispam, se in un numero N di mail analizzate in precedenza, l'utente ha marcato come spam quelle che contenevano, per esempio, la parola "sesso", il filtro dedurrà che la presenza di quella parola innalzi la probabilità che le e-mail contenenti quella parola siano a loro volta spam. In questo modo, il sistema è in grado di adattarsi in maniera dinamica e veloce alle nuove tipologie di spam.

"Ogni evento a cui è attribuita una probabilità è valutabile in base all'analisi degli eventi già verificatesi"

APPROFONDIMENTO TECNICO
Mitigazione degli allegati malevoli

I metodi tradizionali di rilevamento avvengono attraverso signatures e codici di tipi di virus noti che sono già stati rilevati, analizzati e registrati in un database. L'analisi euristica invece è **un metodo che è stato specificatamente progettato per rilevare malware polimorfici**, ovvero una tipologia di virus che si adatta costantemente all'interno di una macchina senza la necessità di una firma specifica.

L'analisi euristica può impiegare due tecniche diverse: statica e dinamica.

EURISTICA STATICA
Prevede la decompilazione, ovvero l'attività di ''ingegneria inversa'' mediante la quale viene ricostruito il codice sorgente a partire da un file eseguibile in linguaggio macchina, e l'esame del suo codice sorgente. Questo codice viene quindi confrontato con virus già noti e presenti nel database euristico. Se una determinata percentuale del codice sorgente corrisponde a qualcosa nel database euristico, il codice viene contrassegnato come possibile minaccia.

APPROFONDIMENTO TECNICO
Mitigazione degli allegati malevoli

EURISTICA DINAMICA

Viene effettuata isolando il programma o il pezzo di codice sospetto all'interno di una sandbox e offre all' antivirus la possibilità di testare il codice e simulare cosa accadrebbe se il file sospetto fosse autorizzato a funzionare. Esamina ogni comando quando viene attivato e cerca eventuali comportamenti sospetti, come l'auto-replica, la sovrascrittura dei file e altre azioni comuni ai malware.

Uno dei potenziali problemi è che deve essere attentamente ottimizzata per fornire il miglior rilevamento possibile di nuove minacce ma senza generare falsi positivi su un codice innocente. Per questo motivo, gli strumenti euristici sono spesso in genere solo un'arma in un sofisticato arsenale di antispam e antivirus.

APPROFONDIMENTO TECNICO
Mitigazione degli allegati malevoli

L'adozione delle sandbox per il riconoscimento dei malware è diventata fondamentale per contrastare gli attacchi mirati. La sandboxing e-mail funziona isolando i file sospetti per osservare e per determinare come si comporta il codice e cosa nasconde al suo interno.

È un ambiente virtuale dove si esegue un'analisi approfondita dei contenuti mettendo in quarantena i file e facendoli detonare senza causare danni reali agli utenti.

Le sandbox tradizionali adottano un ambiente controllato emulando un sistema operativo standard (OS). Le organizzazioni criminali per bypassare questa tecnologia utilizzano le cosiddette sleep evasions inserendo un "timer di spegnimento" per ritardare l'esecuzione del payload nel malware e consentirne l'apertura del file giorni o mesi dopo l'ispezione. Un altro “trick” che utilizzano i malware è la user behaviour per capire se si è all’interno di una sandbox o se vi è la presenza di un utente reale che compie delle azioni. Di conseguenza è necessario dotarsi di sistemi avanzati con nuove funzionalità: le sandbox più avanzate sono basate su una tecnica chiamata emulazione di sistema completa.

APPROFONDIMENTO TECNICO
Mitigazione degli allegati malevoli

La differenza chiave tra le sandbox basate su macchine virtuali e quelle basate su emulatori di codice è che le cosiddette virtual machine, in genere, non virtualizzano completamente la CPU utilizzata per eseguire il codice del malware.
Un emulatore di codice gestisce direttamente ogni istruzione eseguita all'interno del sistema di analisi ed è quindi in grado di manomettere l'esecuzione come vuole il sistema. Ciò avviene in modo completamente trasparente e invisibile al malware sotto analisi.

Ad esempio, il sistema vede quali altri potenziali comportamenti potrebbero essere in agguato nel malware che non sono stati attivati durante l'analisi dinamica, fornendo alla sandbox ulteriori informazioni per classificare un malware.

APPROFONDIMENTO TECNICO
Mitigazione degli allegati malevoli

Soluzioni di Data Loss Prevention prevengono la perdita di dati sensibili nelle e-mail e possiedono funzionalità che facilitano la conformità alle politiche aziendali e alle normative del settore. Risultano utili per individuare e prevenire tentativi di copiare o inviare dati sensibili senza autorizzazione.

Queste soluzioni utilizzano diversi metodi per classificare le informazioni sensibili come la corrispondenza esatta dei dati, parole chiavi e metodi statistici. I sistemi DLP avanzati sfruttano differenti algoritmi pensati per personalizzare i livelli di sicurezza, in modo da monitorare gli accessi e prevenire furti di dati.

Si può decidere a quale livello monitorare la posta elettronica:

- Contenuto
- Header
- Allegati e-mail inoltrate
- Le parole chiave e le espressioni possono essere specificate a livello di gateway, dominio e utente.

Vi è la possibilità di rinforzare le policy DLP (bloccare, porre in quarantena, eliminare, criptare) e attivare un alert per l’IT manager nel caso di invio di informazioni di natura finanziaria all'esterno dell'organizzazione.

APPROFONDIMENTO TECNICO
Awareness e Phishing test

È di fondamentale importanza Investire sull'*awareness* dei dipendenti attraverso training specifici per ridurre il rischio di attacco: il 90% delle compromissioni del perimetro tramite e-mail in azienda è causato dal phishing.
Vi sono diverse tipologie di formazioni da organizzare per approcciare il tema:

1.Bollettini interni settimanali
2.Corsi mensili su argomenti specifici tenuti da esperti
3.Notifiche e aggiornamenti live sugli attacchi

La responsabilità deve essere condivisa tra tutte le persone dell'organizzazione: le aziende possono dotarsi di tutte le tecnologie più sofisticate ma dovranno fare affidamento prima di tutto sulla formazione degli utenti a cui spesso si riferisce come "Human Firewall".

Il phishing test è uno strumento indispensabile per testare la preparazione degli utenti nell'identificare mail anomale.
Simula possibili attacchi creando campagne di phishing innocue: all'interno delle mail sono inseriti link per tenere traccia dell'avvenuto adescamento e dei click dell'utente.

Alla fine dell'attività viene generalmente stilato un report dettagliato e rischedulato un ciclo di formazione di awareness per colmare le lacune dei dipendenti più inclini al phishing.
L'esecuzione di questo test viene suggerita all'inizio di un progetto di sicurezza per comprendere la effettiva consapevolezza degli utenti in azienda.

CONCLUSIONI

Umberto Eco usava scrivere: «per me l'uomo colto è colui che sa dove andare a cercare l'informazione nell'unico momento in cui gli serve».

Questo è ciò che abbiamo cercato di fare con questa ricerca, dare alle persone la consapevolezza che le domande non iniziano e non finiscono nella e-mail che hanno di fronte.

La sicurezza di una organizzazione passa necessariamente dalla preparazione che tutti i suoi elementi hanno nei confronti delle minacce.

SITOGRAFIA

www.gartner.com/en/documents/3883275/fighting-phishing-2020-foresight

https://businessinsights.bitdefender.com/bitdefender-2020-cybersecurity-predictions

www.commissariatodips.it/approfondimenti/phishing/phishing-che-cose/index.html

www.trendmicro.com/it_it/what-is/phishing.html

www.wired.it/internet/web/2014/04/10/come-difendersi-phishing-clicca-qui/

www.hackerwebsecurity.com/spoofing-di-email-url-post-e-non-solo/

www.repubblica.it/tecnologia/sicurezza/2018/05/03/news/40_anni_spam_anniversario_posta_elettronica_email-195334283/

https://www.cybersecurity360.it/nuove-minacce/spear-phishing-e-social-engineering-aumentano-gli-attacchi-targettizati-quali-impatti-per-le-aziende/

https://www.fortinet.com/blog/threat-research/tracking-down-big-phish.html

https://docs.microsoft.com/it-it/microsoft-365/security/office-365-security/anti-spam-protection

SITOGRAFIA

https://www.microsoft.com/security/blog/2019/10/16/top-6-email-security-best-practices-to-protect-against-phishing-attacks-and-business-email-compromise/

https://www.achab.it/achab.cfm/it/blog/prodotti/mdaemon/quali-tecnologie-per-rendere-sicuri-i-propri-messaggi-email

https://docs.microsoft.com/it-it/exchange/antispam-and-antimalware/antispam-protection/antispam-protection?view=exchserver-2019

https://www.bertoldicybersecurity.com/sicurezza-dns-come-configurare-spf-dkim-e-dmarc-per-la-posta-del-tuo-dominio/

https://encyclopedia.kaspersky.it/knowledge/the-evolution-of-spam/

www.isaca.org/resources/isaca-journal/issues/2017/volume-6/evasive-malware-tricks-how-malware-evades-detection-by-sandboxes

www.thesslstore.com/enterprise/email-document-signing-certificates.aspx?utm_source=phishing-ebook&utm_medium=content#parentHorizontalTab1

www.theemaillaundry.com/full-stack-email-security-service/

www.mimecast.com/products/email-security-with-targeted-threat-protection/url-protect/

Entra nel canale Telegram

cybergon.com
cybergon.com/blog
linkedin.com/company/cybergon

CYBERGON
ADVANCING THE STATE OF CYBERSECURITY