UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Campagna di Phishing Sinergia

Gianalberto Cecchini

Sinergia EPC srl

www.sinergia.it

gcecchini@sinergia.it

Martedì 19 settembre 2023

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Phishing

Definizione di phishing

Il phishing è un tentativo **fraudolento** di **ottenere informazioni sensibili** ingannando la vittima attraverso la ricezione di una comunicazione **apparentemente affidabile**.

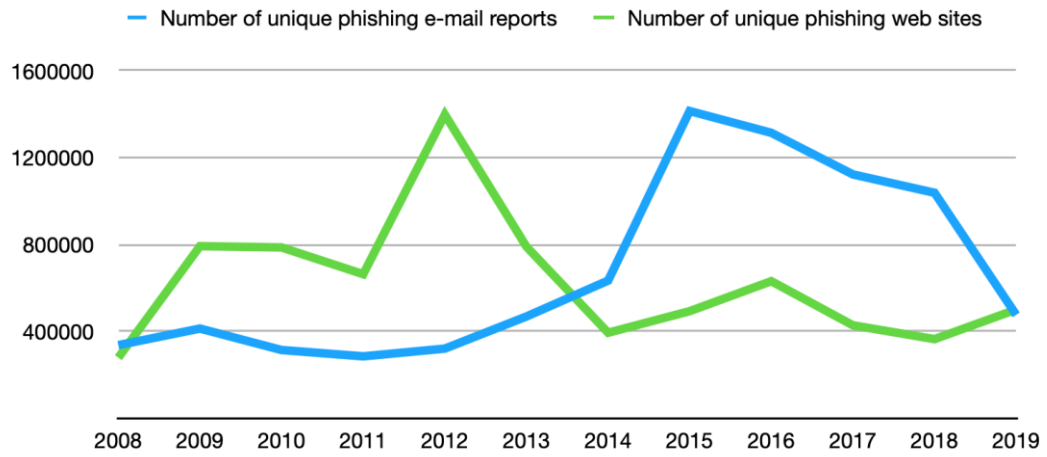
Generalmente in un attacco di phishing su larga scala vengono carpiti **nomi utenti, indirizzi email, password e dettagli delle carte di credito**.

Per attacchi di phishing **mirati** nei confronti di utenti o aziende l'obiettivo potrebbe essere quello di carpire **altre informazioni riservate**.

L'ingegneria sociale è la principale tecnica utilizzata per ingannare l'utente in un tentativo di phishing. Un attaccante **deve sapere fingere ed ingannare** la vittima dell'attacco al fine di carpire informazioni utili.

Un po' di numeri

L'Anti-Phishing Working Group (APWG) rilascia ogni trimestre un report contenente il rapporto sulle attività di phishing analizzate riportando il numero univoco di email e di 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**.

Un po' di numeri

Una ricerca di **PhishLabs** evidenzia che:

- la qualità delle singole campagne sia aumentata: difatti **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
- Il **56,51%** delle email inviate nel 2021 contengono spam: +4% rispetto al 2020. I principali paesi che hanno inviato email di spam sono Cina (21,26%), USA (14,39%) e Russia (5,21%)
- Il paese maggiormente colpito da campagne malevoli è la Germania (11,86%), seguita dalla Russia e dal Vietnam (5,77%) poi l'Italia (5,57%)
- Il **20,17%** degli Italiani ha ricevuto un attacco di phishing nel corso del 2020.
- 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%).

Tipologia di attacchi

- La tradizionale campagna di phishing viene effettuata su una ampia platea di utenti e senza una verifica accurata poiché l'intento è quello di acquisire un grande numero di informazioni sensibili.
- Il **Spear Phishing** è una campagna più accurata e mirata nei confronti di un singolo individuo o una società. Questa tipologia di attacchi prevede un'attenta analisi del target e le informazioni raccolte vengono sfruttate nella campagna malevola per rendere la comunicazione più attendibile ed incrementare la probabilità di successo
- Il **Clone Phishing** 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, una variazione del "**Man in the Middle**".

Tipologia di attacchi

- 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.

Vettori di attacco

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.

SMS

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. Il messaggio solitamente:

- riporta un sito web fraudolento molto simile all'originale
- impersona il nominativo o numero di telefono di un'altra persona o soggetto, avvalorando maggiormente la comunicazione.

Vettori di attacco

Social Network

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.

Instant Message

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.

Voce

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.

Campagna Sinergia

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

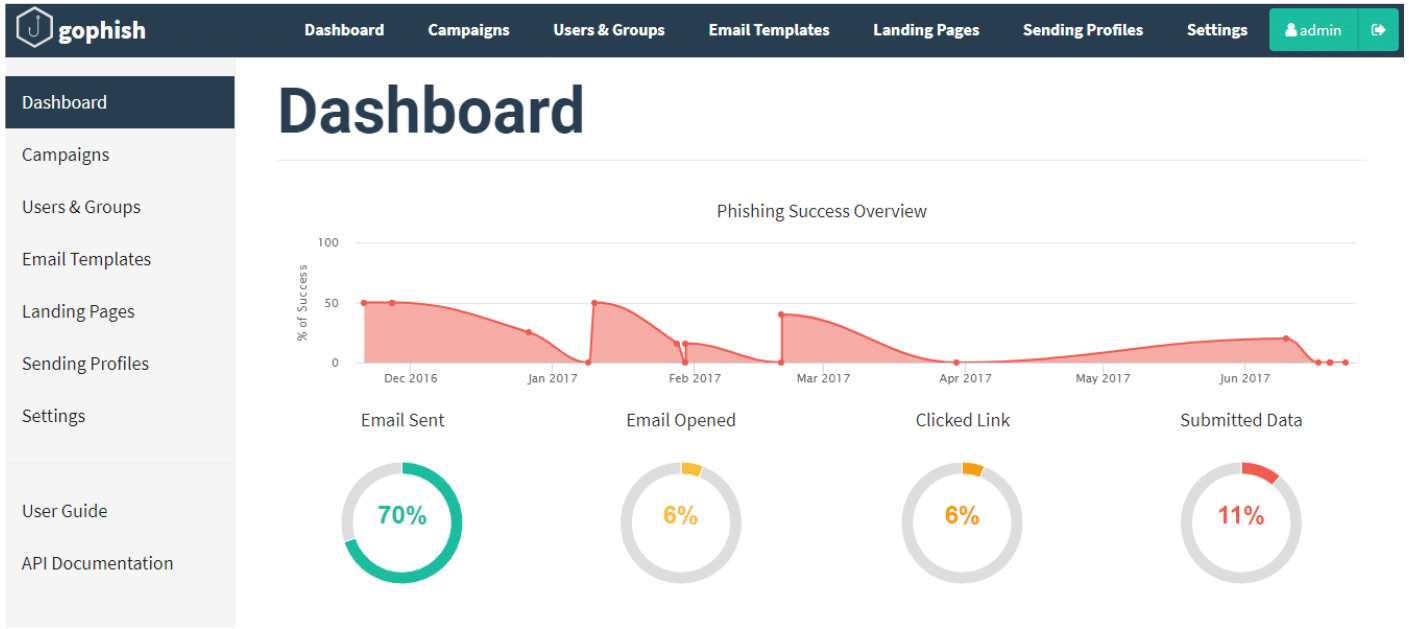
Scenario

- Modalità di attacco ibrida tra lo "*Spear Phishing*" ed il "*Business Email Compromise*" impersonando l'Amministratore Delegato della società.
- La scelta è stata dettata dal fatto che quest'ultimo ricopre anche il ruolo di responsabile IT, dunque delle email aventi come oggetto un argomento riguardante alcune configurazioni del server di posta sarebbero apparse verosimili.
- Il dominio scelto per questa campagna è **sinegia.it** molto simile a quello originale (sinergia.it) mancante tuttavia della lettera "*r*".
- Dopo aver ricavato un numero sufficiente di indirizzi email tramite alcuni servizi come https://phonebook.cz è stata creata la lista finale composta da 25 destinatari.

Software

GoPhish

Framework open source per la creazione e la simulazione di campagne di phishing concepito allo scopo di valutare quale possa essere l'esposizione di una data azienda a questa tipologia di attacco informatico.



Software

Evilginx2

Framework sviluppato per eseguire test di sicurezza e per scopi didattici ed è dedicato a tutti i professionisti della cybersecurity che vogliono mettere alla prova i protocolli e le contromisure da implementate nei sistemi dei loro clienti.

Questo tool agisce come una sorta di proxy tra un browser Web e un sito Web coinvolto da un'attività di phishing con l'obiettivo di sottrarre credenziali di accesso sfruttando i cookie di sessione, in modo da bypassare anche il maggior livello di protezione offerto dalla verifica a due fattori.

Un attacco di tipo man-in-the-middle avviene quando un'entità terza ritrasmette o altera la comunicazione tra due parti che credono di comunicare direttamente tra di loro, come avviene appunto nel caso di un browser e un server Web.

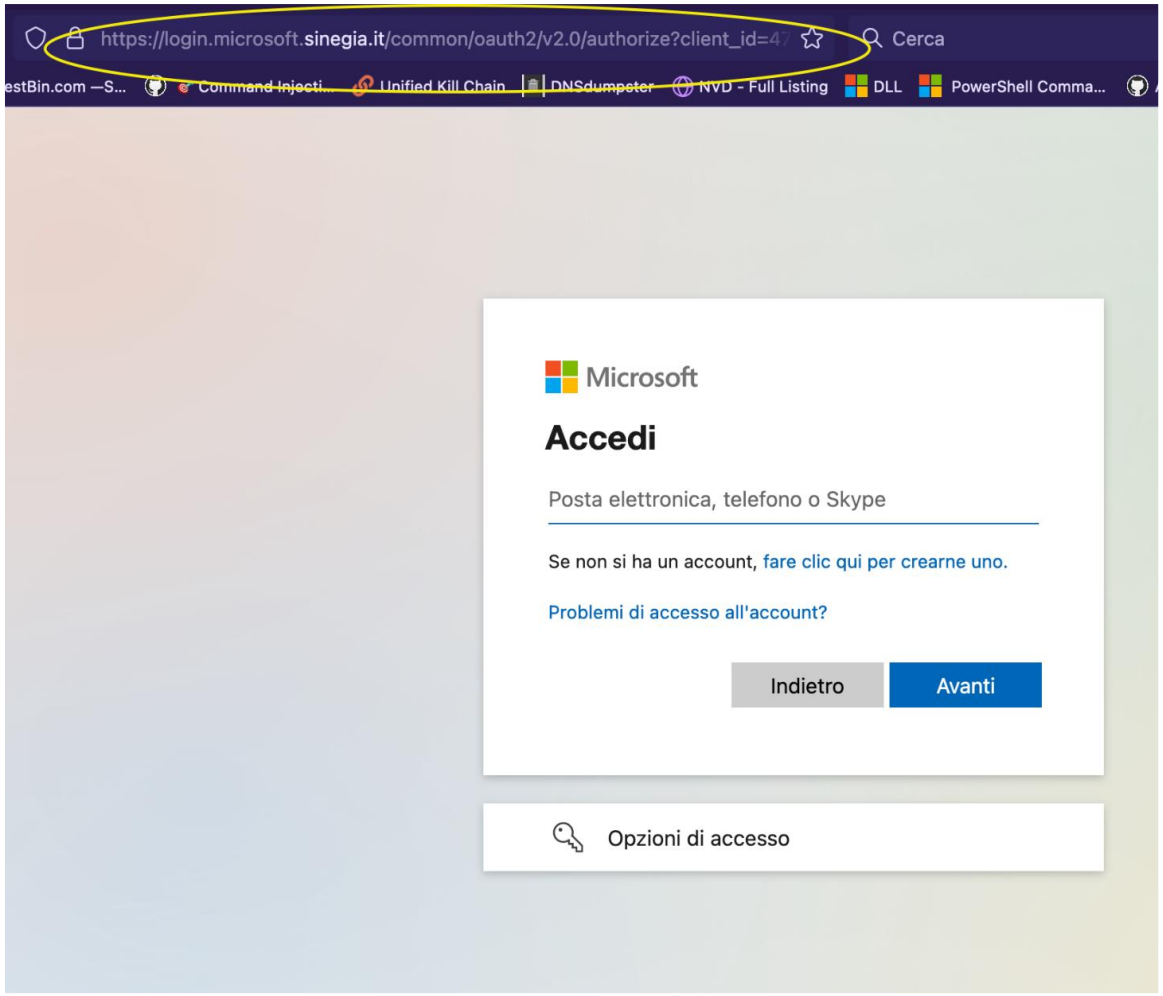
Campagna

1. Creazione pagina web

Sinergia si avvale dei servizi offerti dalla suite di **Microsoft Office 365**, motivo per il quale è stato deciso di indirizzare gli utenti presso un pannello di login della suite

Gli strumenti utilizzati **NON** replicano una pagina di login fittizia bensì quella che è stata presentata all'utente è **ESATTAMENTE** la vera pagina di login di Microsoft Office 365 con un differente URL.

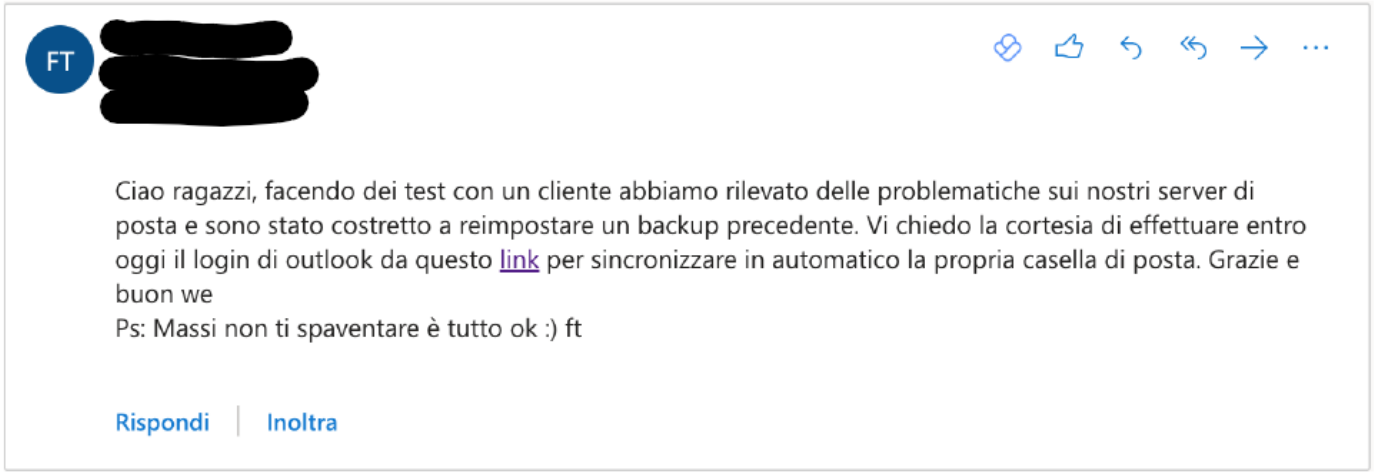
I software malevoli sono però in ascolto pronti ad intercettare le credenziali di accesso.



Campagna

2. Testo della email

In questo caso specifico, trattandosi di una simulazione di un attacco mirato (*spear phishing*), il messaggio aveva lo scopo di emulare il più possibile le dinamiche comunicative aziendali



È stato predisposto anche un server di posta elettronica atto a ricevere eventuali risposte con lo scopo di evitare che i dipendenti avessero potuto ricevere, nel momento in cui avessero eventualmente risposto alla mail di phishing, un messaggio di "*Mail Delivery Failure*"

Reazione del personale

- La presenza di gruppi Whatsapp ha fatto sì che i dipendenti più sospettosi potessero comunicare le proprie perplessità in tempo reale, avvertendo in contemporanea tutti i destinatari.

- La divisione tecnologica della società si è subito mossa per cercare il server di provenienza identificando il server di test.

- In ogni caso, i dipendenti di hanno avuto un comportamento corretto, analizzando la email e non cliccando compulsivamente, confrontandosi ed avvisando il titolare.

- Selezionare e formare il personale vuol dire goderne i suoi frutti anche e soprattutto in situazioni come questa che possono potenzialmente mettere a rischio un’intera azienda.

Analisi

Il software di monitoraggio ha rilevato che soltanto in pochi hanno aperto il link allegato alla mail ed appena un solo dipendente ha effettivamente portato a completamento la procedura di login. Questo può essere considerato oggettivamente un ottimo risultato unito all'approccio collaborativo che ha contribuito alla realizzazione del risultato.

id	phishlet	username	password	tokens	remote ip
52	outlook			none	79.34.105.117
53	outlook			none	5.88.70.114
54	outlook			none	2.45.212.206
55	outlook			none	176.32.28.93
56	outlook			none	109.112.0.167
57	outlook	[redacted]	[redacted]	captured	[redacted]
58	outlook			none	85.18.87.105

Tuttavia, nonostante l'esito di questo test sia decisamente positivo, è sufficiente un solo elemento per mettere a rischio l'intera infrastruttura IT aziendale.

Contromisure preventive

Honey User

Si tratta di creare un utente fittizio ed inserirlo nel proprio sito web così come nella propria pagina Linkedin. Nessuno invierà email a quell'utente perché tutti all'interno dell'azienda sapranno essere un'esca. Il reparto IT può monitorare questo indirizzo, dipanando in maniera automatica degli alert da inviare a tutta l'azienda nel momento in cui un messaggio di posta dovesse essere ricevuto nella casella dell' honey user.

Spoofpoint

Creare una lista di domini simili al proprio (es sinegia.it, sìnergia.it, etc) e periodicamente effettuare un whois per ogni dominio in cerca di record MX. Nel caso in cui ne trovasse, vorrebbe dire che qualcuno sta predisponendo o ha già predisposto una campagna di phishing a vostro svantaggio.

Contromisure preventive

Awareness

Il cerchio si chiude con la formazione. Le campagne di phishing sono uno strumento efficace se effettuate con regolarità. Il mondo del cybercrime è in costante evoluzione e le tecniche mutano e si perfezionano ogni giorno. Il vettore di attacco non è più soltanto confinato alle email ma comprende sms, app di messaggistica, telefonate. Il training dei propri dipendenti dovrebbe abbracciare anche queste tipologie di phishing per far sì che la loro preparazione sia al passo coi tempi.

Conclusioni

La campagna di phishing effettuata per testare il livello di preparazione dei dipendenti di Sinergia è da considerarsi oggettivamente **positiva**.

Nonostante ciò, l'invito è quello di **non abbassare la guardia**.

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

È pertanto fondamentale **formare** i dipendenti nel riconoscere una comunicazione illegittima o i meccanismi consolidati di questa tipologia di frode.

UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Campagna di Phishing Sinergia

Grazie!

Martedì 19 settembre 2023

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection