UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO

DIPARTIMENTO
DI INFORMATICA

RELAZIONE DEL PROGETTO
DI
SICUREZZA INFORMATICA
A.A. 2019/2020

E-Mail Phishing con SocialFish

24 GENNAIO 2020

Team: ***Giant Steps***
Autori: *Matteo Luceri*
Vincenzo Conte
Marco Grassi

SocialFish

GIANT STEPS

Sommario

1 Introduzione

1.1 Il team e il progetto

Giant Steps è un gruppo di studenti del terzo anno dell'Università degli studi "Aldo Moro" del corso di laurea Informatica e Comunicazione Digitale con sede a Taranto, composto da Matteo Luceri, Vincenzo Conte e Marco Grassi.

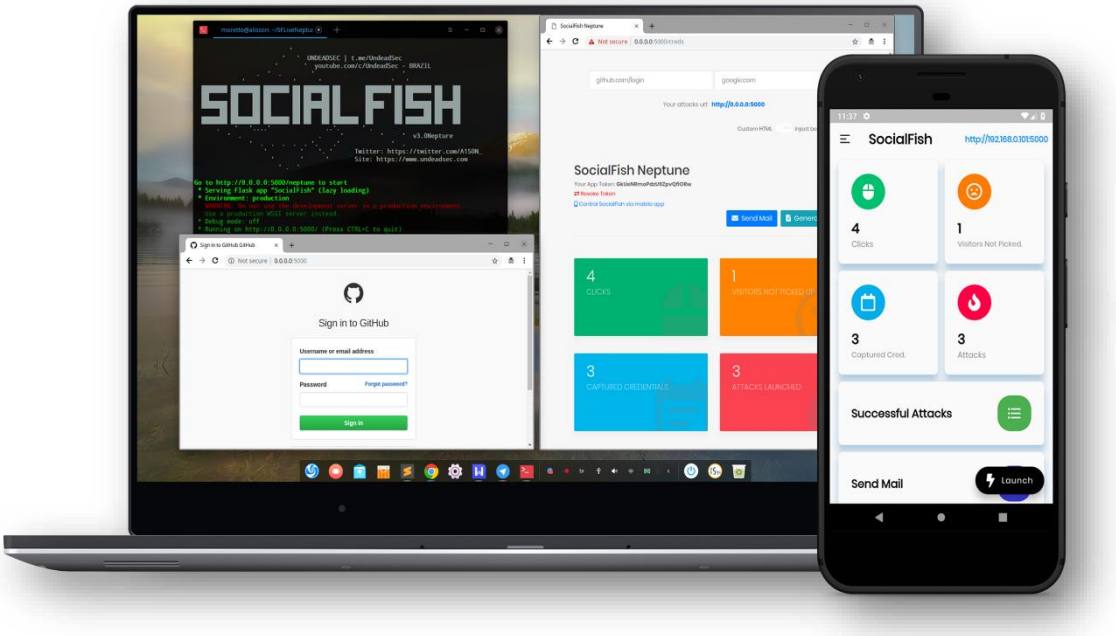
Il progetto verte sull'analisi di un ipotetico attacco mediante il tool SocialFish.
I riferimenti per documentazione e turorial al tool sono disponbibili su GitHub all'indirizzo: https://github.com/UndeadSec/SocialFish.

1.2 Contesto

Si è deciso di realizzare un attacco che ha l'obiettivo di sfruttare le vulnerabilità di un utente che si interfaccia al web.
Nello specifico si realizzerà un attacco di e-mail phishing, usando il tool all-in-one SocialFish, il quale, clonerà una pagina di login (LinkedId, Facebook, Twitter, ecc...), genererà un link corrotto, e permetterà di inoltrare tale link alla vittima, tramite e-mail.

Lo scopo è quindi quello di prelevare le credenziali di accesso della vittima.

Per gestire l'attacco, SocialFish mette a disposizione una dashboard online.



Infatti sarà possibile - avviato il server con SocialFish – gestire gli attacchi in atto e leggere tutte le credenziali prelvate dagli utenti che hanno "abboccato".

1.3 Scenario

Lo scenario che vogliamo rappresentare si basa su due concetti fondamentali.

Il primo è costituito dalla natura stessa del web.
La crescita esponenziale dell'informatica, del web e delle sue implicazioni nella vita reale ha portato ad un altrettanto crescente ignoranza dell'utenza che si affaccia a risorse o servizi disponibili liberamente sul web.

L'utente medio ed attivo su internet , nel 2020, guarda video su YouTube, visita quotidianamente social network, gestisce il proprio account di home banking , ecc. Ma quanti di questi utenti sono realmente consapevoli dell'uso che fanno di tali risorse e servizi? Quanti sanno delle informazioni e dei dati che rilasciano?

Numerosi si affacciano al web come se stesserò usando una black box ! Un input, un output e nulla di più !

Ci siamo quindi chiesti quanto questo divario tecnologico-digitale influisca e costituisca di fatto una vulnerabilità evidente e potenzialmente pericolosa per un utente.

Il secondo concetto costituente dell'attacco è il così detto *trust*.
Posto il digital divide, se pur parziale, dell'utente medio, un'e-mail di phishing risulta facilmente "individuabile" da un servizio di posta elettronica e/o da un utente.
Il *trust* , la "fiducia", di un sito a cui siamo particolarmente affezionati, o che conosciamo come serio od affidabile, costituisce un ulteriore e possibile vulnerabilità sfruttabile per un attaccante.
Un'e-mail scritta bene, simile in tutto e per tutto ad un'e-mail di un sito spesso visitato, può essere facilmente recepita dall'utente come fidata !

Si prevede quindi un scenario in cui, Luca Rossi, un ex lavoratore per un ditta, la Woody Arredamenti, (ditta emergente nel settore di arredamenti fatti a mano e venduti online) è stato licenziato ingiustamente.
Luca vuole vendicarsi facendo un danno all'immagine dell'azienda, e , per fare ciò, è intenzionato a prelevare le credenziali di LinkedIn di utenti di spicco dell'azienda, conscio della loro scarsa conoscenza informatica.

Tramite una minima operazione di ingeneria sociale, chiarendo il background delle vittime, e conoscendo le loro scarse conoscenze informatiche, Luca individua diverse potenziali vittime.
Fatto ciò, genera un clone della pagina di accesso di LinkedIn , ed invierà via e-mail il link corrotto.

Se gli utenti "abboccheranno" Luca potrà accedere,(se è anche fortunato) con le medesime credenziali, agli indirizzi e-mail e/o agli account delle vittime ed effetturare potenziali danni all'azienda con operazioni di raccolta e rilascio di informazioni sensibili, o con operazioni di carattere distruttivo.

2 Kill Chain

Riepilogo Kill Chain

KILL CHAIN		
Red Team		Blue team
Il potenziale phisher determina il prossimo obiettivo, clona il link creandone uno corrotto, crea l'elenco di e-mail.	Reconnaissance	Introdurre sistemi di autenticazione multi-fattore.
Il phisher crea l'e-mail di phishing.	Weaponization	Adottare policy che neghino all'utente la possibilità di apertura di mail sospette, dovendone prima verificare l'autenticità del mittente.
Il tentativo di e-mail di phishing viene inviato alla persona o alle persone nell'elenco e-mail. L'email di phishing utilizza informazioni ingannevoli all'interno dell'e-mail per ingannare l'utente	Delivery	Introdurre software o servizi di filtro spam o mail malevole.
La vittima fa clic sui collegamenti dannosi nell'e-mail	Exploit	Introdurre *Security Awareness Training*, ovvero corsi di sicurezza anti-phishing per i dipendenti.
La vittima immette i dati personali nel sito dannoso	Installation	
Il sito dannoso invia le informazioni all'attaccante	Command & Control	
L'attaccante utilizza le informazioni rubate per commettere crimini informatici	Action	Modificare le credenziali di accesso, sia "username" che "password", di tutti i dipendenti attaccati.

2.1 Reconnaissance

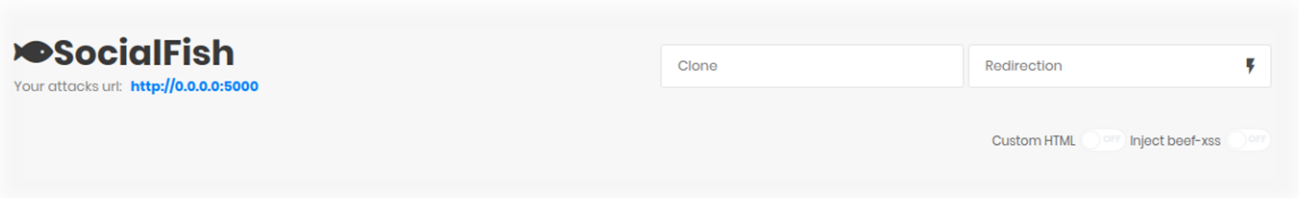
Fase molto importante in quanto è dedicata alla raccolta delle informazioni sull'obiettivo. È una fase che determina il successo o l'insuccesso delle fasi successive e quindi del risultato finale.

2.1.1 Red Team

Il potenziale phisher determina il prossimo obiettivo, clona il sito e crea l'elenco di e-mail.

L'attacco in oggetto è calibrato per macchine aventi una connessione ad Internet, e per l'utenza avente un indirizzo e-mail.

L'attaccante individua le vittime (fase di social engineering) , gli indirizzi e-mail da attaccare (fase di discover) e la piattaforma social da attaccare.
Fatto ciò, individua il sito o i siti web da clonare, per generare la pagina fittizia da cui si ruberanno le informazioni.



Le tecniche MITRE ATT&CK coinvolte sono:

- Conduct social engineering, (PRE-ATT&CK, ID T1249) , per la fase di social engineering,
- Discover target logon/e-mail address format (PRE-ATT&CK , ID T1255), per la fase di discover.
- Mine social media , (PRE-ATT&CK , ID T1273) , per la scelta della piattaforma web da clonare.

2.1.2 Blue Team

Introdurre sistemi di autenticazione multi-fattore.

Per difendersi da attacchi di individui non autorizzati sarà necessario utilizzare la tecnica del multi-factor authentication. (MITRE&ATTACK). Le politiche aziendali prevedono tecniche di autenticazione a due fattori (il login verrà confermato tramite codice ricevuto via sms, per esempio), le tecniche utilizzate per evitare attacchi indesiderati.

Le tecniche MITRE ATT&CK coinvolte sono:

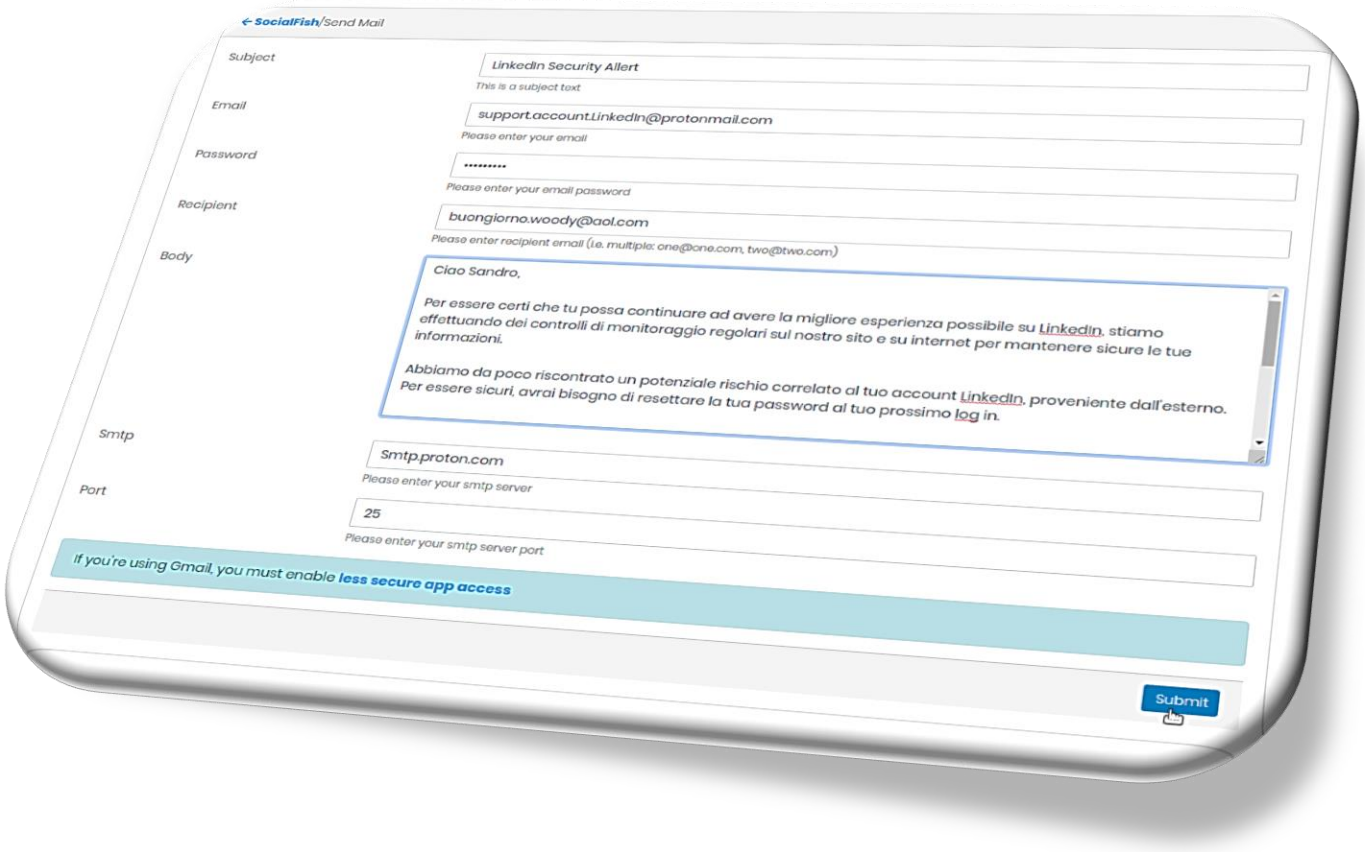
- Multi-factor Authentication, (Enterprise, ID M1032).

2.2 Weaponization

Fase che riguarda la preparazione dell'e-mail di phishing .

2.2.1 Red Team

Il phisher crea l'e-mail di phishing.
L'email di phishing utilizza informazioni ingannevoli al suo interno per ingannare l'utente.



L'attaccante scrive l'e-mail, inserendo il link corrotto, usando il tool SocialFish.

Le tecniche MITRE ATT&CK coinvolte sono:

- Obtain templates/branding materials, (PRE-ATT&CK , ID T1281) , per la creazione di e-mail credibili contenenti loghi o template del brand,

2.2.2 Blue Team

Adottare policy che neghino all'utente la possibilità di apertura di mail sospette, dovendone prima verificare l'autenticità del mittente.

Per evitare attacchi di tipo phishing, i dipendenti prima di visionare i messaggi ricevuti tramite indirizzi di posta elettronica aziendale, dovranno verificare l'autenticità dei messaggi, accertandosi che gli autori delle suddette mail siano attendibili, inoltre su tutti i dispositivi verrà installato un antivirus regolarmente aggiornato e corredato di opportuni pacchetti addizionali atti alla prevenzione di attacchi di tipo phishing e similari.

Le tecniche MITRE ATT&CK coinvolte sono:

- Antivirus / Antimalware, (Enterprise , ID M1049) .

2.3 Delivery

Fase che riguarda l'invio dell'e-mail di phishing creata nella fase precedente.

2.3.1 Red Team

Il tentativo di e-mail di phishing viene inviato alla persona o alle persone nell'elenco e-mail.

L'attaccante invia l'e-mail usando il tool SocialFish.

Le tecniche MITRE ATT&CK coinvolte sono:

- Spearphishing Link, (Enterprise , ID T1192) , tecnica che descrive gli attacchi che si manifestano tramite l'invio di link corrotti o malevoli;
- Standard Application Layer Protocol, (Enterprise , ID T1071), tecnica che descrive i protocolli di comunicazione standard (SMTP);

2.3.2 Blue Team

Introdurre software o servizi di filtro spam o mail malevole.

Adottare filtri spam integrati nei servizi di posta elettronica oppure software (per esempio, Microsoft's phishing filter).

Le tecniche MITRE ATT&CK coinvolte sono:

- Filter Network Traffic, (Enterprise, ID M1037), tecnica che descrive modalità di filtraggio del flusso di rete;

2.4 Exploit

Fase in cui l'attaccante clicca il link corrotto.

2.4.1 Red Team

La vittima fa clic sui collegamenti dannosi nell'e-mail

La vittima, fidandosi del contenuto dell'e-mail, apre il link corrotto.

Le tecniche MITRE ATT&CK coinvolte sono:

- User Execution (Enterprise , ID T1204) , tecnica che descrive l'esecuzione, da parte dell'utente, di attachment o link malevoli.

2.4.2 Blue Team

Introdurre Security Awareness Training, ovvero corsi di sicurezza anti-phishing per i dipendenti.

L'introduzione di training formativi dei dipendenti, con lo scopo di ridurre gli errori umani e consentire un riconoscimento di link corrotti (nel nostro caso http://0.0.0.0/5000) da parte degli utenti.

Le tecniche MITRE ATT&CK coinvolte sono:

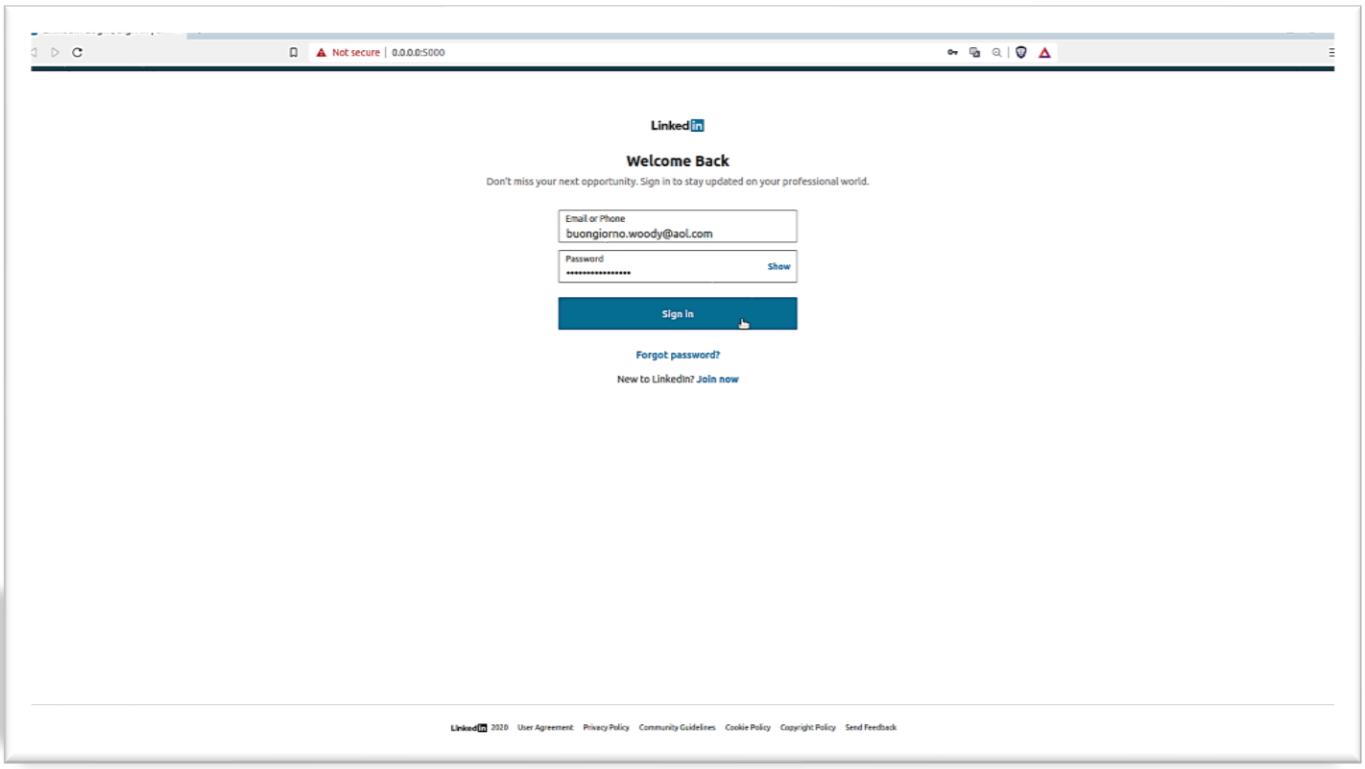
- User Training (Enterprise , ID M1017) , tecnica che rappresenta le fasi di training degli utenti su rischi e possibili vulnerabilità.

2.5 Installation

2.5.1 Red Team

La vittima immette i dati personali nel sito dannoso.

La vittima convinta che sia la pagina di accesso originale, immette le proprie credenziali di accesso.



Le tecniche MITRE ATT&CK coinvolte sono:

- Input Capture, (Enterprise , ID T1056) , tecnica che descrive la fase di cattura di input immesso da un utente;

2.5.2 Blue Team

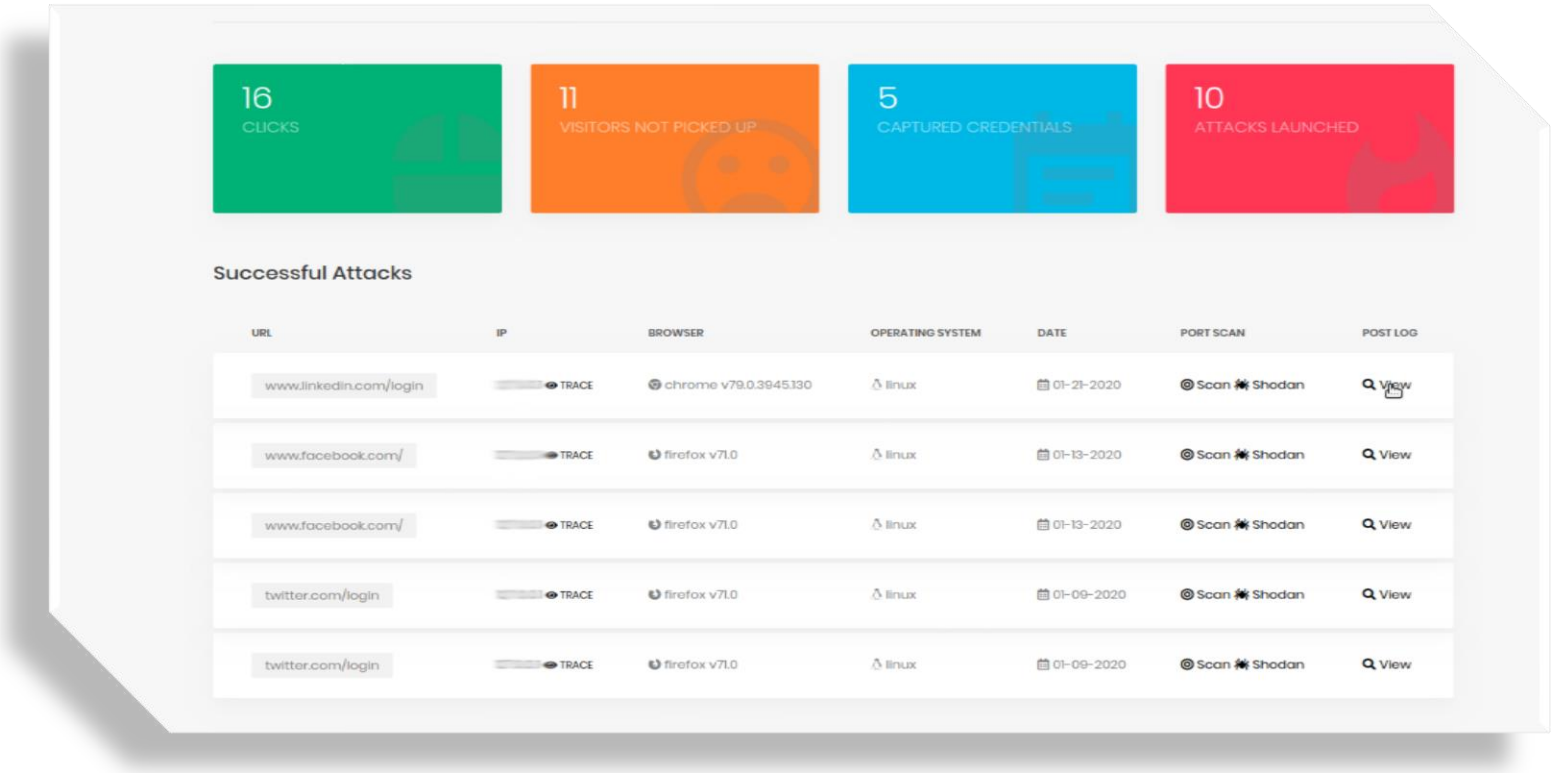
2.6 Command & Control

In questa fase l'attaccante assume il controllo da remoto del sistema compromesso.

2.6.1 Red Team

Il sito dannoso invia le informazioni all'attaccante

Le credenziali inserite saranno inviate al phisher, che potrà consultare facilmente gli attacchi in atto, dalla sua dashboard, con SocialFish.



Le tecniche MITRE ATT&CK coinvolte sono:

- Automated Collection, (Enterprise , ID T1119) , tecnica che descrive la fase di collezione di dati automatica;
- Standard Application Layer Protocol, (Enterprise , ID T1071), tecnica che descrive i protocolli di comunicazione standard;

2.6.2 Blue Team

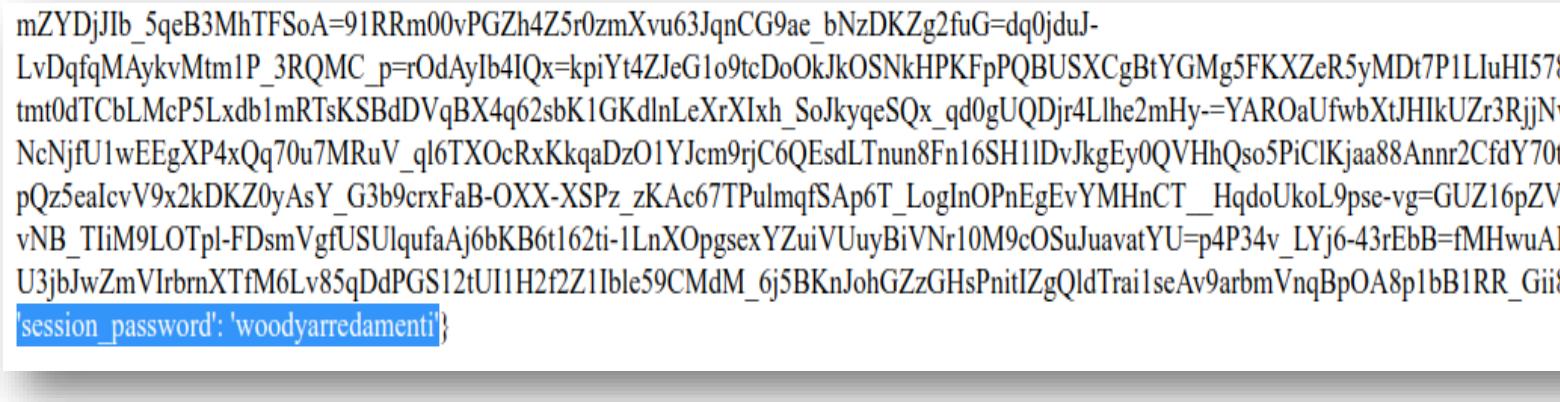
2.7 Action

Gli hacker eseguono le operazioni a loro utili per rubare informazioni sensibili e sferrano attacchi ad altri dispositivi di rete.

2.7.1 Red Team

L'attaccante utilizza le informazioni rubate per commettere crimini informatici

Il phisher, ormai in possesso delle credenziali di accesso, può effettuare ulteriori crimini informatici, accedendo ad altri siti, o eliminando/distruggendo dati e/o accounts.



Le tecniche MITRE ATT&CK coinvolte sono:

- Valid Accounts, (Enterprise , ID T1078), tecnica che descrive la fase in cui si prende possesso di credenziali di accesso a un servizio o di accesso di un utente;
- Stored Data Manipulation, (Enterprise , ID T1492), tecnica che descrive la fase in cui possono inserire, distruggere o manipolare dati di accesso.

2.7.2 Blue Team

Modificare le credenziali di accesso, sia "username" che "password", di tutti i dipendenti attaccati.

Al fine di contenere i danni, si attueranno azioni di salvaguardia degli account compromessi, con il cambio e il rinnovo delle credenziali di accesso.

Le tecniche MITRE ATT&CK coinvolte sono:

- User Account Management, (Enterprise , ID M1018), tecnica che descrive le fasi di creazione, modifica e gestione dei permessi relativa agli account utente.