S5L5 Progetto settimanale

*(Tutto ciò rappresentato per iscritto e per immagini è stato svolto su rete locale su un uno solo dispositivo, non sono state coinvolte persone terze in questo **scenario simulato**)*

Contesto scenario:

Lo scenario rappresentato, vede come **vittima** un utente di **CryptoForest.com** (una piattaforma per investimenti di crypto), ricevente di un **email falsa** apparentemente ufficiale. Il contento dell'email ha come avviso urgente riguardante l'accesso sospetto sul suo account. L'attaccante sfrutta l'**ingegneria sociale**, infondendo **ansia** e **paura** alla vittima, così da ricavare informazioni essenziali come **email** e **password**. La vittima inconsapevole ed ignorante riguardo la **metodologia di phishing**, inserisce le sue credenziali dentro il **sito clonato**, che arriveranno successivamente all'attaccante.

Fase di preparazione:

L'attaccante dopo aver comprato un **dominio web** ed un **email** simili a quelle di Crypto Forest**,** tramite il tool **setToolKit** crea il sito clone, collegandolo alla sua macchina.

Inoltre tramite strumenti molto potenti come **Maltego** e **theHarvester** ricava dati sensibili della vittima, scoprendola in possesso di un'**ingente quantità di bitcoin** all'interno del suo account, inoltre viene a sapere del suo **nome** ed **indirizzo email**, queste informazioni, **importantissime**, permetteranno all'attaccante di creare un contenuto per l'email, **perfetto** e **indistinguibile** da quello originale agli occhi della vittima.

L'attaccante si è avvalso anche di **ChatGPT**, per la creazione del contenuto dell'email, qui sotto vediamo l'esempio:

Da: support@crypto-forest.com
A: john.white@example.com
Oggetto: Azione richiesta: Problema tecnico sul tuo account Crypto Forest

---

Gentile John White,

Durante il recente aggiornamento della nostra piattaforma, abbiamo rilevato un **problema tecnico** che potrebbe influenzare i fondi del tuo account Crypto Forest. Per evitare inconvenienti, ti chiediamo di confermare i dettagli del tuo account, assicurandoci così che i tuoi fondi rimangano al sicuro.

Dettagli del problema:
Un'anomalia è stata rilevata durante la sincronizzazione del portafoglio collegato al tuo account, causando una **temporanea limitazione dell'accesso ai tuoi fondi**.

Passo da seguire:
Per risolvere la situazione e assicurarti un accesso continuo al tuo account, ti invitiamo a cliccare sul link sottostante e completare la procedura di verifica:

Verifica il tuo Account Crypto Forest

Importante: Ti preghiamo di completare la verifica entro le prossime 12 ore. Se non effettui questa procedura, l'accesso al tuo account potrebbe essere limitato per garantire la sicurezza dei tuoi fondi.

Se hai domande o desideri maggiori informazioni, contattaci all'indirizzo support@crypto-forest.com.

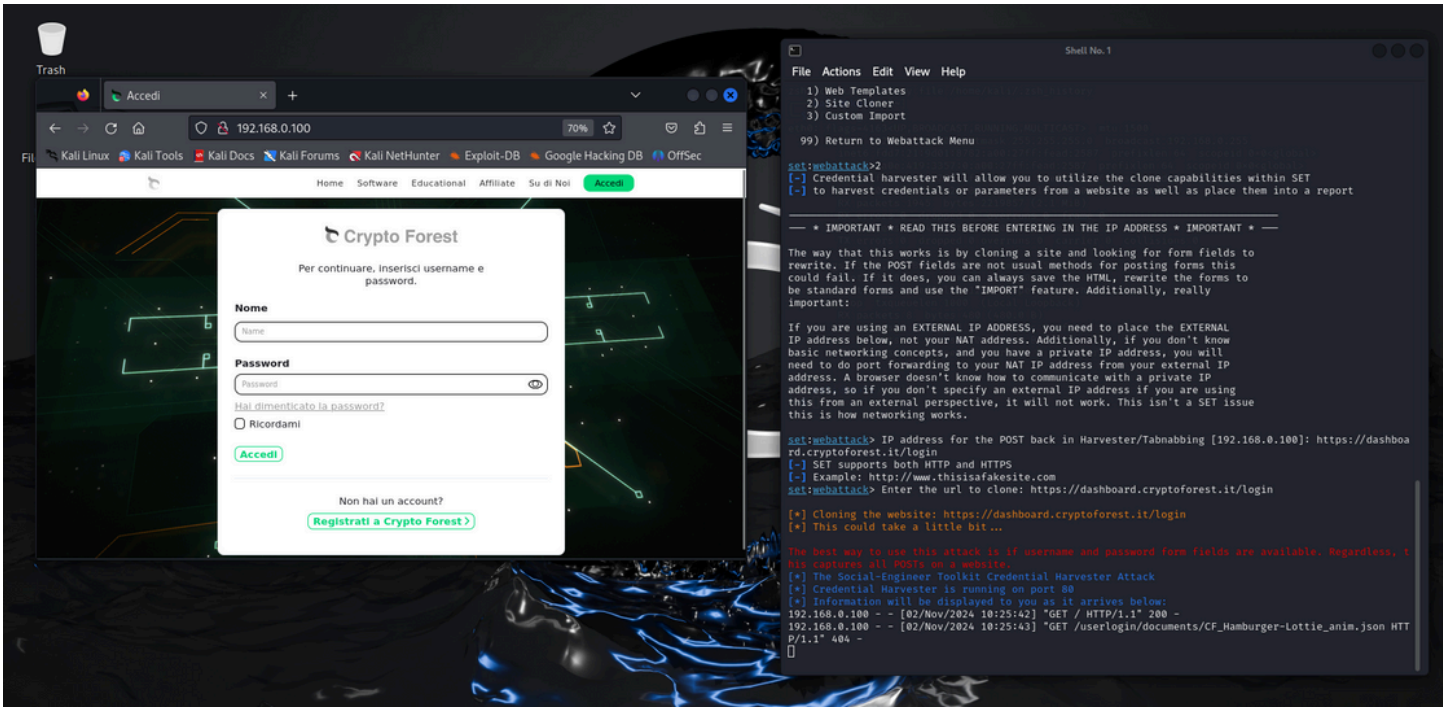
Ci scusiamo per l'inconveniente e ti ringraziamo per la collaborazione,
Il Team di Crypto Forest

Nel link **“Verifica il tuo Account Crypto Forest”**, ci sarà il dominio dell’attaccante con il **sito clone**, dal quale li informazioni inserite arriveranno direttamente alla macchina del malintenzionato.

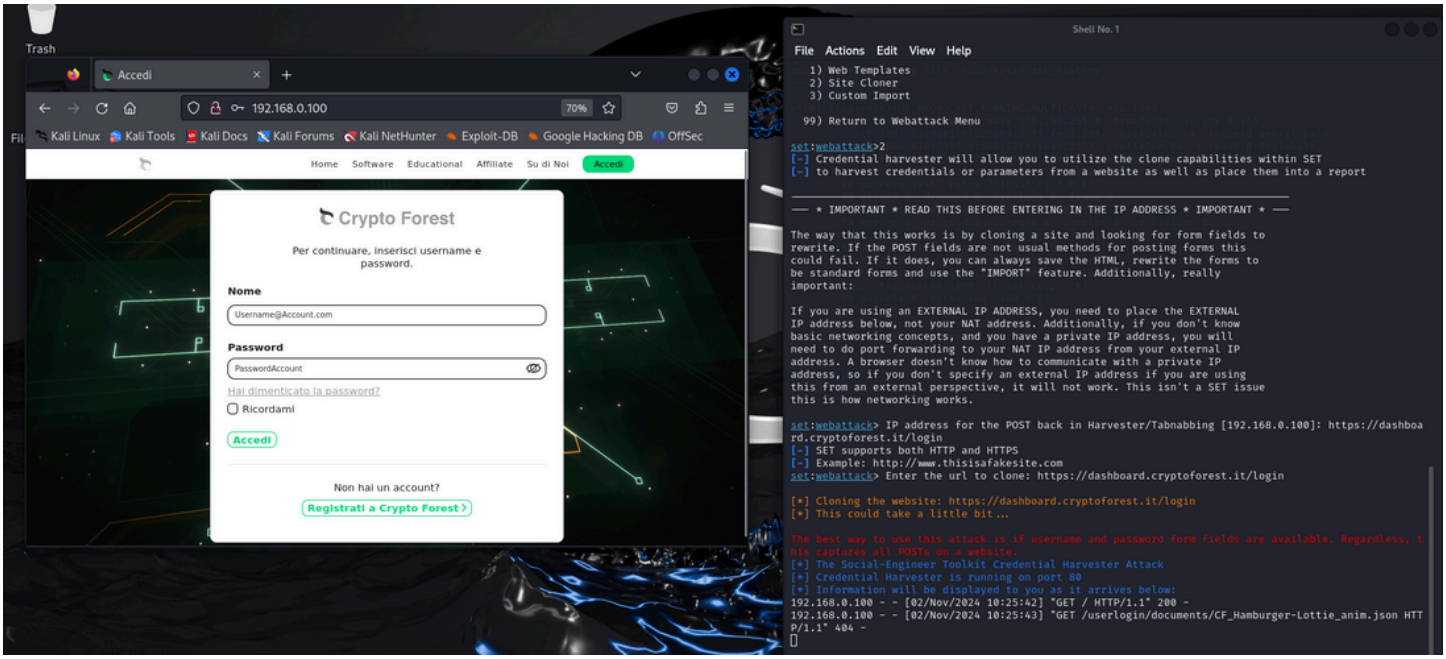
Fase di attacco:

Una volta completata la fase di preparazione, l’attaccante **invia** l’email malevola alla vittima, una volta **“abboccato“** l’utente verrà scosso dall’**ansia** e della **paura**, vedendo i suoi fondi a rischio. Si precipiterà nel sito:

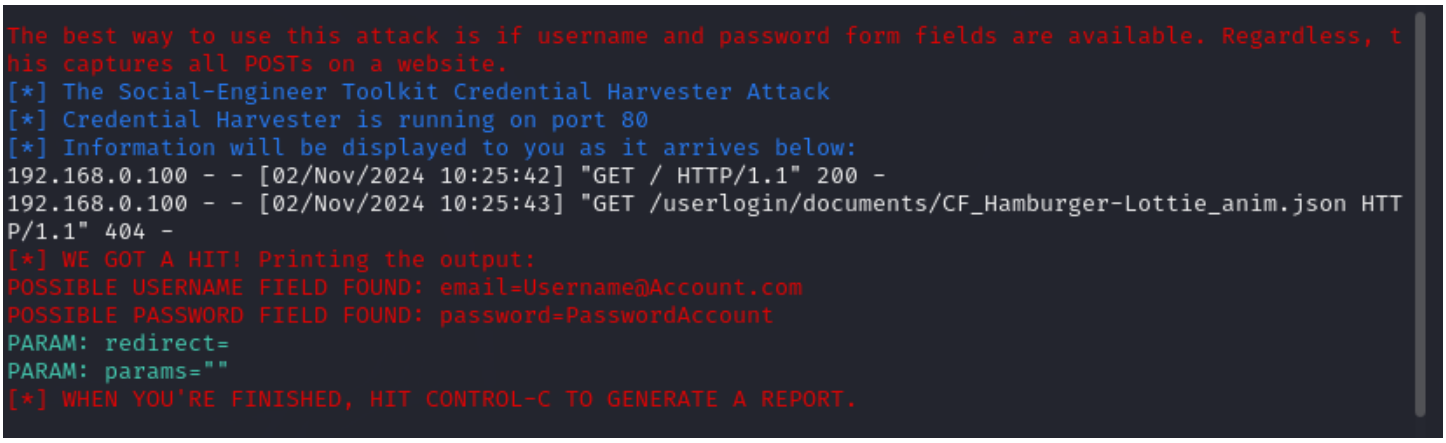
Da lì l'attaccante già saprà che la vittima è dentro, **vedendo l'indirizzo IP collegato**:



Successivamente l'utente **digiterà le credenziali**:



Una volta **premuto invio**, non succederà nulla agli occhi della vittima, ma sulla macchina dell'attaccante verranno visualizzati **nome utente** o **email** e **password**.



Da questo momento, se la vittima non ha ancora **abilitato** la **verifica a 2 fattori** o altri tipologie di sicurezza per il suo account, l'attaccante avrà completo accesso al suo account, rubandone i fondi.

Scenario comune:

In questo caso l'attaccante è stato furbo, rendendo il contenuto dell'email più dettagliato possibile, perché riguardante un solo soggetto, ma comunemente questi tentativi di phishing vengo fatti su **larga scala**. Dove troviamo:

- **Errori grammaticali e di ortografia** ("una problema tecnico", "indisponibilitá", "limitazzioni").
- **Mancanza di personalizzazione**: la comunicazione si rivolge a "Gentile cliente" invece che al nome di John White.
- **Link sospetto**: il dominio del link contiene errori e non è quello ufficiale ("crypto-f0rest-support.com" invece di "crypto-forest.com").
- **Indirizzo email del mittente sospetto**: "supp0rt@crypto-forest.com" con un zero ("0") al posto della "o".

Gentile cliente,

Abbiamo rilevato una problema tecnico nel tuo conto su Crypto Forest. Questo può causare **indisponibilitá temporanea** dei tuoi fondi fino a quando non verificheremo i dati del tuo conto. É importante che tu agisca presto per evitare limitazzioni sul tuo account.

Dettagli del problema:
Alcune informazioni del tuo portafoglio risultano mancanti. Per confermare il tuo conto, ti chiediamo di seguire il link qui sotto e accedere al tuo pannello.

Verifica tuo conto Crypto Forest

Nota Importante: Se non completi la procedura entro 24 ore, il tuo conto potrebbe essere limitato e i fondi non accessibili.

Per assistenza o domande, scrivi a supp0rt@crypto-forest.com.

Scusa per il inconveniente,
Team di suportto Crypto Forest

Conclusioni:

Gli attacchi di phishing sfruttano la psicologia dell'**urgenza** e della **paura** per indurre gli utenti a **compiere azioni rapide**, come cliccare su link sospetti o inserire dati sensibili su siti non sicuri. Le email di phishing, come quella simulata di Crypto Forest, sono progettate per sembrare autentiche, ma presentano spesso **errori** e **dettagli** che possono rivelarne la **natura fraudolenta**.

Segnali di Allerta di una Email di Phishing:

1. **Errori grammaticali e di ortografia**: Gli attacchi di phishing spesso contengono errori di scrittura, frasi incoerenti o termini non professionali;
2. **Indirizzi email sospetti**: Controlla attentamente l'indirizzo email del mittente, che può avere caratteri sostituiti o leggermente modificati (come "supp0rt" invece di "support");
3. **Assenza di personalizzazione**: Le email autentiche spesso utilizzano il nome dell'utente; un saluto generico come "Gentile cliente" può indicare un tentativo di phishing;

4. **Link ingannevoli**: Prima di cliccare, passa il mouse sopra i link per visualizzare l'URL. I siti falsi possono sembrare simili a quelli originali, ma contengono spesso errori, simboli o numeri insoliti.

Come Difendersi dal Phishing:

1. **Non cliccare sui link sospetti**: In caso di dubbi, evita di cliccare sui link nell'email e accedi al sito ufficiale digitandolo direttamente nella barra del browser;
2. **Verifica l'autenticità dell'email**: Contatta direttamente il servizio clienti di Crypto Forest (o della piattaforma interessata) utilizzando i contatti ufficiali reperibili sul loro sito web;
3. **Attiva l'autenticazione a due fattori (2FA)**: Questa misura di sicurezza aggiuntiva può proteggere il tuo account anche nel caso in cui le credenziali venissero compromesse;
4. **Non condividere mai informazioni personali tramite email**: I servizi ufficiali non richiedono mai credenziali o dettagli sensibili via email;
5. **Segnala il tentativo di phishing**: Se ricevi un'email sospetta, segnala immediatamente il tentativo di phishing alla piattaforma interessata. Molti servizi offrono un'email specifica per raccogliere queste segnalazioni.