Malicious PDF: Implementazione di una Macro per il Download di un Virus

I. Introduction

Il progetto si propone di realizzare un documento PDF malevolo con l'implementazione di alcune caratteristiche specifiche. L'obiettivo principale è dimostrare le potenzialità degli attacchi basati su file PDF con funzionalità dannose e comprendere le implicazioni in termini di sicurezza informatica.

Gli obiettivi specifici del progetto includono:

- Creazione di un PDF malevolo: Il primo obiettivo è quello di sviluppare un documento PDF che contenga un file Microsoft Word incorporato. Il PDF sarà progettato per ingannare l'utente e indurlo a eseguire azioni che attivano funzionalità dannose.
- Implementazione di una macro: Il file Microsoft Word incorporato conterrà una macro che si attiva automaticamente all'apertura del documento. La macro sarà progettata per scaricare un malware da un server command and control (C2).
- Incorporazione di un codice JavaScript: Il documento PDF conterrà anche un codice JavaScript che verrà eseguito quando l'utente apre il documento. Questo codice avrà il compito di salvare il file Microsoft Word incorporato e di avviare l'esecuzione della macro.
- Inganno dell'utente: Il file Microsoft Word sarà progettato per indurre l'utente a consentire l'esecuzione delle macro, ad esempio fornendo istruzioni fuorvianti o utilizzando tecniche di ingegneria sociale.

Attraverso il completamento di tali obiettivi, il progetto mira a fornire una dimostrazione pratica delle potenzialità degli attacchi basati su documenti PDF malevoli e delle vulnerabilità che possono essere sfruttate nel contesto della sicurezza informatica.

Per lo sviluppo del progetto è stato creato un ambiente di sviluppo basato sulla virtualizzazione utilizzando il software VirtualBox. All'interno di questo ambiente sono state configurate due macchine virtuali che rappresentano l'attaccante e la vittima.

- **Macchina virtuale dell'attaccante (Kali Linux):**
  La prima macchina virtuale è stata configurata utilizzando il sistema operativo Kali Linux, una distribuzione specializzata per il penetration testing e l'analisi della sicurezza. Sono stati installati e configurati gli strumenti necessari per eseguire le operazioni di attacco come la gestione del server C2. Questa macchina virtuale rappresenta l'entità malintenzionata che conduce l'attacco.
- **Macchina virtuale della vittima (Windows):**
  La seconda macchina virtuale è stata configurata con il sistema operativo Windows, creando un ambiente che simula un utente ignaro che apre il documento PDF malevolo. La macchina virtuale è stata predisposta con le impostazioni appropriate per emulare un ambiente tipico di una vittima potenziale. Durante le fasi di test, verranno monitorate le azioni della vittima e gli effetti dell'attacco, compreso il download e l'esecuzione del malware. Questa macchina virtuale rappresenta il bersaglio dell'attacco.

II. Creazione del server C2

Per realizzare il server C2, è stato utilizzato il linguaggio di programmazione Python insieme alla libreria http.server. Questa libreria fornisce un'implementazione base per la gestione dei server HTTP in Python.

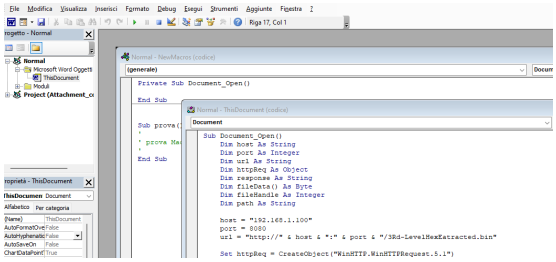
Il server C2 è stato configurato per utilizzare una connessione HTTP per avviare la comunicazione tra il server e la macro in Word. Una volta avviato, il server rimane in ascolto sulla porta specificata e attende che il documento PDF malevolo faccia una richiesta GET per scaricare il file.

Quando il server C2 riceve una richiesta GET per il percorso specificato, ad esempio '/satan.bin', viene avviata la gestione della richiesta. Il server invia una risposta con il file come allegato da scaricare. Una volta che il server C2 è in esecuzione, rimane costantemente in ascolto per eventuali richieste GET provenienti dal documento PDF malevolo.

III. Creazione del file Word con la macro

Le macro di Word offrono un potente strumento per automatizzare compiti ripetitivi e complessi all'interno dei documenti Microsoft Word. Una macro è essenzialmente una sequenza di comandi e istruzioni che possono essere registrati o scritti manualmente per eseguire azioni specifiche all'interno di un documento Word. Le macro consentono di automatizzare processi, applicare formattazione personalizzata, manipolare dati. Per creare e gestire le macro in Microsoft Word, viene utilizzato il linguaggio di scripting VBA (Visual Basic for Applications). VBA è basato sul linguaggio Visual Basic e offre una vasta gamma di funzionalità e librerie specifiche per l'automazione delle applicazioni Microsoft Office, tra cui Word. Con VBA, è possibile accedere e manipolare gli oggetti all'interno di Word, come paragrafi, tabelle, immagini

e altro ancora. È possibile creare loop, condizioni, definire variabili, gestire eventi e utilizzare molte altre costruzioni del linguaggio per creare macro complesse e personalizzate. Le macro sono state introdotte come un meccanismo legittimo per automatizzare le operazioni all'interno delle applicazioni Microsoft Office, tuttavia, negli ultimi anni, questa funzionalità è stata utilizzata per scopi malevoli. Le macro malevole si sono diffuse ampiamente grazie alla facilità con cui possono essere integrate in documenti comuni come file Word o fogli di calcolo Excel. Questi documenti vengono spesso inviati tramite email o distribuiti tramite siti web compromessi, sfruttando l'ingegneria sociale per convincere gli utenti ad aprirli e abilitare le macro.



L'obiettivo della macro implementata è di attivarsi automaticamente all'apertura del file Word e procedere con il download ed esecuzione di un virus. Per raggiungere questo obiettivo, è stato scritto il codice VBA nel modulo ThisDocument del documento Word. La funzione Sub DocumentOpen() all'interno di questo modulo viene eseguita automaticamente non appena il file Word viene aperto, permettendo l'esecuzione del codice VBA contenuto in essa.

Il codice VBA si connette al server C2 utilizzando una richiesta HTTP per scaricare un file binario malevolo. Prima di tutto, vengono impostate le variabili host, port e url per specificare l'indirizzo IP del server C2, la porta su cui il server è in ascolto e l'URL del file binario da scaricare. Queste informazioni consentono al codice di stabilire una connessione verso il server C2. Una volta configurata la connessione, il codice invia la richiesta al server. Nel caso in cui la risposta abbia avuto successo, il codice memorizza il corpo della risposta del server, ovvero il file binario, nella variabile response e nell'array di byte fileData. Questi dati rappresentano il contenuto del file binario scaricato dal server C2. Una volta scaricato il file dal server lo salvo sulla macchina vittima ed essendo il file un eseguibile windows cambio la sua estensione.

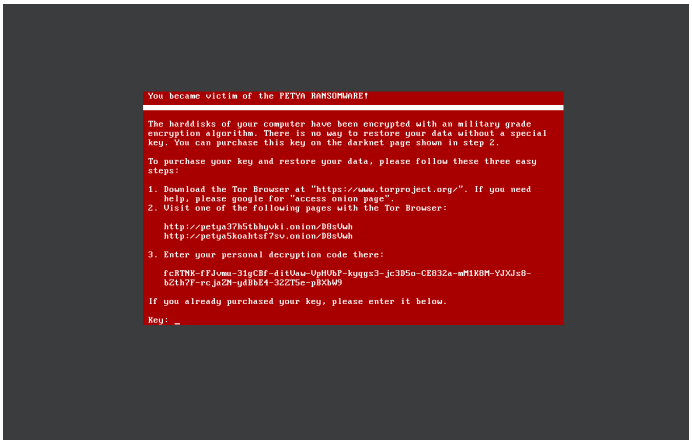
```
Dim objShell As Object
Set objShell = CreateObject("WScript.Shell")
objShell.Run "cmd /c C:\Users\User\
Desktop\virus.exe", 1, True
```

A questo punto il virus è stato scaricato sulla macchina della vittima. La funzione quindi apre una shell di windows ed esegue il file che è stato appena scaricato.

Questo approccio funziona nel caso in cui sulla macchina windows non siano presenti antivirus e che windows defender sia disabilitato. altrimenti non sarebbe possibile eseguire il file in qanto verrebbe risconosciuto come un eseguibile malevolo.

IV. IL VIRUS

Il Petya Ransomware è un noto malware che è emerso per la prima volta nel 2016. Si è diffuso ampiamente e ha causato notevoli danni in tutto il mondo. A differenza di molti altri tipi di ransomware, che si limitano a crittografare i file degli utenti, il Petya ha implementato una funzionalità particolare chiamata "disk-level encryption" (crittografia a livello di disco). Questa caratteristica gli ha conferito un potenziale distruttivo significativo. Il Petya è stato sviluppato per approfittare delle vulnerabilità presenti nei sistemi operativi Windows, sfruttando i punti deboli nella sicurezza per infiltrarsi nelle reti aziendali. Una volta all'interno di un sistema, il malware si propaga rapidamente attraverso la rete, infettando i dispositivi collegati e criptando i file presenti sui dischi rigidi.



Una delle peculiarità del Petya è la sua capacità di compromettere il Master Boot Record (MBR) del sistema. Questo permette al ransomware di avviarsi prima del sistema operativo e di bloccare completamente l'accesso al computer dell'utente. Dopo aver crittografato i file dell'utente, il malware richiede un riscatto per fornire la chiave di decrittografia e ripristinare l'accesso ai dati.

V. CREAZIONE DEL PDF E JAVASCRIPT

Per incorporare un file word all interno di un pdf ho utilizzato Adobe Acrobat Reader in quanto è uno dei programmi piu usati per la modifica dei file pdf ed è presente sulla maggior parte dei computer windows. Il file word viene salvato con l estensione ".docx" e non ".docm" che è l estesione che permette l uso di macro, in quanto per ragioni di sicurezza Adobe Acrobat Reader non permette di scaricare file attaccati a un pdf che possono eseguire codice. Aquesto punto devo incorporare nel pdf del codice javascript per far si che quando la potenziale vittima una volta aperto il pdf scarichi ed esegua automaticamente il file di word attivando cosi la macro che infetterà il sistema con il virus. Adobe Acrobat Reader permette di eseguire codice javascript ma non all apertra del pdf ma associato ad altre azioni come la pressione di un bottone. Per eseguire il codice javascript all apertura del pdf ho usato JS2PDFInjector un programma che utilizza le API di Adobe Acrobat Reader e permette di incorporare del codice javascript

in un pdf. Il codoce javascript per prima cosa mostrera una finestra di dialogo per ingannare l utente ad abilitare le macro per poter visualizzare correttamente il file, in questo modo il virus potra essere scaricato, a quel punto il codice controlla che il file pdf abbia degli attachment e se li ha li salva sulla macchina della vittima e li apre. in questo modo una volta aperto il file file pdf verrà scaricato il file word e la macro al suo interno eseguita infettando così la vittima.