Consegna S11L5
Mirabella Francesco

Malware Analysis Progetto S11-L5

Sommario

Traccia

Con riferimento al codice presente nelle slide successive, rispondere ai seguenti quesiti:

Spiegate, motivando, quale salto condizionale effettua il Malware.

Disegnare un diagramma di flusso (prendete come esempio la visualizzazione grafica di IDA) identificando i salti condizionali (sia quelli effettuati che quelli non effettuati). Indicate con una linea verde i salti effettuati, mentre con una linea rossa i salti non effettuati. Quali sono le diverse funzionalità implementate all'interno del Malware?

Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

Cos’è un Malware

Un malware, o “software malevolo”, è un termine generico che descrive un programma o un codice dannoso che mette a rischio un sistema. Questi sono ostili, invasivi e volutamente maligni, cercano di invadere, danneggiare o disattivare computer, sistemi, reti, tablet e dispositivi mobili, spesso assumendo il controllo parziale delle operazioni del dispositivo. Proprio come l’influenza, interferiscono con il loro normale funzionamento.

Lo scopo dei malware è lucrare illecitamente a spese degli utenti. Sebbene i malware non possano danneggiare gli hardware fisici di un sistema o le attrezzature di rete, possono rubare, criptare o eliminare i dati, alterare o compromettere le funzioni fondamentali di un computer e spiare le attività degli utenti senza che questi se ne accorgano o forniscano alcuna autorizzazione.

I malware possono rivelarsi attraverso tutta una serie di comportamenti anomali. Ecco alcuni indizi che segnalano la presenza di un malware nel sistema:

Il computer funziona più lentamente. Uno dei principali effetti dei malware è la riduzione della velocità del sistema operativo, sia nella navigazione su internet che nel semplice utilizzo delle applicazioni.

Un’ondata di irritanti annunci pubblicitari, che non dovrebbe comparire, riempie lo schermo. La presenza di pop-up imprevisti è il sintomo tipico di un’infezione malware.

Il sistema continua a chiudersi, bloccarsi o mostrare una schermata blu di errore (BSOD), che talvolta viene visualizzata sui dispositivi Windows in seguito a un errore irreversibile.

Il termine malware indica qualsiasi tipo di software creato per danneggiare o sfruttare altri componenti software o hardware2. Contrazione di “malicious software” (software dannoso), malware è un termine collettivo utilizzato per descrivere virus, ransomware, spyware, Trojan e qualsiasi altro tipo di codice o software creato con intenti dannosi. È proprio l’intento dannoso a caratterizzare la definizione di malware: lo scopo del malware è il danno che può infliggere a un computer, un sistema informatico, un server o una rete.

Tutti i virus sono malware, ma non tutti i tipi di malware sono virus. I virus sono un tipo di malware che si auto-replica inserendo il proprio codice in altri file o programmi, diffondendosi poi da un dispositivo infettato a un altro. Per riconoscere se un’infezione è causata da un altro tipo di malware o da un virus, è necessario osservarne il funzionamento. Se il software dannoso non usa altri programmi per replicare se stesso e diffondersi, non si tratta di un virus.

Gli attacchi malware possono violare le password deboli, penetrare in profondità nei sistemi, diffondersi attraverso le reti e interferire con le attività quotidiane di un’organizzazione o di un’azienda. Altri tipi di malware possono bloccare file importanti, inondarti di annunci, rallentare il computer o reindirizzarti a siti Web dannosi. Il malware è alla base della maggior parte degli attacchi informatici, comprese le violazioni dei dati su larga scala che portano a furti di identità e frodi di ampia portata. I malware sono anche responsabili di attacchi ransomware che causano danni per milioni di dollari. Gli hacker indirizzano gli attacchi malware contro individui, aziende e persino governi.

Tipi di analisi Malware

L’analisi del malware è il processo di comprensione del comportamento e dello scopo di un file o URL sospetto1. Ci sono principalmente tre tipi di analisi del malware:

Analisi statica: Questo tipo di analisi non richiede che il codice venga effettivamente eseguito. Invece, esamina il file alla ricerca di indizi di intenti nocivi. Può essere utile per identificare infrastrutture, librerie o file compressi dannosi.

Tuttavia, un malware sofisticato potrebbe includere comportamenti di runtime dannosi che possono non essere rilevati.

Analisi dinamica: Questo tipo di analisi esegue il codice dannoso sospetto in un ambiente sicuro chiamato sandbox. Questo sistema chiuso consente ai professionisti della sicurezza di osservare il malware in azione senza il rischio che possa infettare il proprio sistema o sfuggire alla rete aziendale.

Analisi ibrida: Questo tipo di analisi include sia tecniche statiche che dinamiche.

Ogni tipo di analisi ha i suoi vantaggi e svantaggi, e la scelta del tipo di analisi da utilizzare può dipendere dal contesto specifico.

Cos'è un salto condizionale?

Un salto condizionale è un'istruzione in un programma che permette di passare da un punto all'altro del codice a seconda che una certa condizione sia vera o falsa. Questo è un concetto fondamentale nella programmazione e si trova in tutte le lingue, dai linguaggi ad alto livello come Python o Java, ai linguaggi assembly utilizzati per scrivere malware.

Nel contesto dei malware, un salto condizionale può essere utilizzato per vari scopi. Ad esempio, un malware potrebbe utilizzare un salto condizionale per decidere se eseguire o meno una certa funzione a seconda delle condizioni del sistema in cui si trova. Questo potrebbe includere controlli sul sistema operativo, sulla presenza di specifici software di sicurezza, o su altre caratteristiche del sistema.

Cos'è IDA PRO

IDA Pro è uno strumento di analisi del codice binario di alta qualità, utilizzato da analisti di software, ingegneri inversi, analisti di malware e professionisti della sicurezza informatica1. Ecco alcune delle sue caratteristiche principali:

Disassemblatore: IDA Pro è in grado di creare mappe dell'esecuzione per mostrare le istruzioni binarie effettivamente eseguite dal processore in una rappresentazione simbolica (linguaggio assembly).

Debugger: IDA Pro supporta più target di debug e può gestire applicazioni remote. Ha la capacità di debug cross-platform.

Interattivo: IDA Pro permette all'analista umano di sovrascrivere le sue decisioni o di fornire suggerimenti, così da lavorare in modo più intuitivo con il disassemblatore e analizzare il codice binario.

Integrazioni: IDA Pro funziona su tutte le piattaforme standard e gestisce più processori.

Architettura plug-in aperta: Le funzionalità di IDA possono essere facilmente estese mediante l'uso di plug-in programmabili.

IDA Pro è diventato lo standard de facto per l'analisi del codice ostile, la ricerca di vulnerabilità e la convalida commerciale.

Svolgimento Esercizio

Panoramica sul codice

L'analisi del codice evidenzia l'esistenza di comandi di controllo del flusso. Questi comandi permettono al malware di fare scelte operative basate sullo stato attuale dei registri del processore. Queste scelte sono fondamentali per l'esecuzione condizionata di segmenti di codice che potrebbero essere dannosi. Questa capacità di prendere decisioni rende il malware più versatile e potenzialmente più pericoloso.

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Salto condizionale del Malware

Nel contesto dell'analisi del malware, il flusso di esecuzione del codice può essere rappresentato come un diagramma di flusso. Questo diagramma può essere suddiviso in blocchi di istruzioni e nodi decisionali.

Inizio dell'Esecuzione:

Il diagramma inizia con un nodo di partenza che rappresenta l'inizio dell'esecuzione del malware.

Primo Blocco di Istruzioni:

Un nodo operativo rappresenta l'istruzione mov EAX, 5, dove viene inizializzato il registro EAX.

Il flusso prosegue con un nodo decisionale che mostra il risultato del cmp EAX, 5, che verifica se EAX contiene il valore 5.

Primo Nodo Decisionale e Salto Condizionale: Il flusso del codice inizia con un nodo decisionale che verifica se il valore del registro EAX è uguale a 5. A seconda del risultato di questo confronto, il flusso si biforca in due percorsi:

- Se EAX non è uguale a 5, il flusso segue una linea verde che indica un salto alla Tabella 2 (jnz 0040BBA0).
- Se EAX è uguale a 5, il flusso prosegue lungo una linea rossa verso il successivo blocco di istruzioni.

Secondo Blocco di Istruzioni: Il flusso del codice prosegue con un'operazione di incremento del registro EBX (inc EBX). Successivamente, un altro nodo decisionale verifica se il valore di EBX è uguale a 11 (cmp EBX, 11).

Secondo Salto Condizionale: A seconda del risultato del confronto, il flusso si divide nuovamente:

- Se EBX è uguale a 11, il flusso segue una linea verde che indica un salto alla Tabella 3 (jz 0040FFA0).
- Se EBX non è 11, il flusso prosegue lungo una linea rossa.

Creazione del Diagramma: Per creare il diagramma di flusso, si possono utilizzare strumenti di modellazione come Microsoft Visio, Lucidchart o simili. È importante adottare convenzioni standard per i diagrammi di flusso, come l'uso di rettangoli per le operazioni, rombi per le decisioni e linee direzionali per indicare il flusso. Inoltre, si possono utilizzare colori distinti (verde e rosso) per rappresentare i percorsi del flusso basati sui risultati dei confronti.

Analisi del Diagramma: Il diagramma di flusso rivela i meccanismi decisionali del malware e fornisce una base visiva per l'analisi del suo comportamento. Questa rappresentazione grafica può aiutare gli analisti di sicurezza a identificare rapidamente i punti critici del codice, a comprendere le condizioni che attivano funzioni dannose e a preparare strategie di difesa basate sui percorsi di esecuzione del malware.

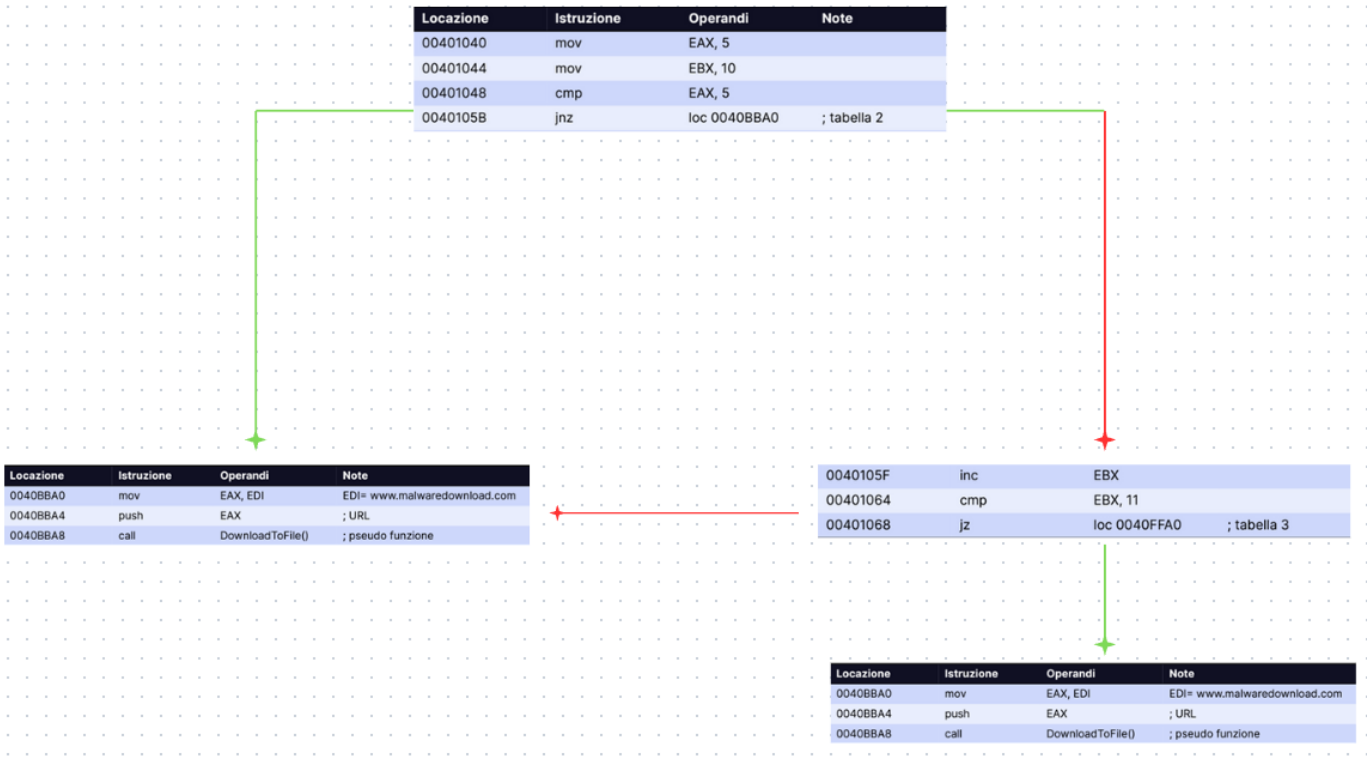
Conclusione: La creazione di un diagramma di flusso accurato è un passo fondamentale nell'analisi del malware. Il diagramma serve come documento di riferimento che facilita la comprensione tecnica e supporta l'elaborazione di contromisure. Gli analisti di sicurezza dovrebbero utilizzare il diagramma come punto di partenza per un'indagine approfondita e per la comunicazione chiara dei rischi e delle soluzioni ai membri del team di sicurezza e ai decisori aziendali.

Diagramma di flusso

Il diagramma di flusso è uno strumento grafico fondamentale per l'analisi del codice, specialmente per la rappresentazione del comportamento di malware sofisticati. Il diagramma facilita la comprensione del flusso decisionale del malware, che si basa su condizioni di esecuzione dipendenti dallo stato dei registri del processore.

Guida Dettagliata alla Creazione del Diagramma di Flusso Il diagramma di flusso del malware dovrebbe illustrare visivamente il flusso logico del codice, basato sulle istruzioni di salto condizionali. Ecco una guida passo-passo per la creazione del diagramma:

1. **Identificare le Istruzioni di Salto Condizionali**: Queste istruzioni determinano il flusso del codice. Identificarle aiuta a capire come il malware reagisce a diverse condizioni.
2. **Rappresentare le Condizioni di Esecuzione**: Ogni istruzione di salto condizionale dovrebbe avere un percorso per "vero" e uno per "falso". Questi percorsi rappresentano le diverse azioni che il malware può intraprendere.
3. **Includere lo Stato dei Registri del Processore**: Lo stato dei registri del processore può influenzare le decisioni del malware. Rappresentare questi stati può aiutare a capire come il malware si comporta in diverse situazioni.
4. **Usare Simboli Standardizzati**: Utilizzare simboli standardizzati per rappresentare diverse parti del codice, come le istruzioni di salto, le operazioni e le funzioni.
5. **Creare Percorsi Chiari e Leggibili**: Assicurarsi che il diagramma sia facile da seguire. Utilizzare frecce per indicare il flusso del codice e mantenere il layout il più pulito possibile.



Funzionalità implementate all'interno del Malware

Introduzione:

L'indagine sui segmenti di codice ha rivelato alcune funzionalità cruciali del malware in esame. Queste funzionalità mostrano un comportamento malevolo, tipicamente utilizzato per compromettere i sistemi, sottrarre dati o infliggere altri tipi di danni.

Funzionalità Identificate Scaricamento di File Malevoli *Descrizione*: Il malware sembra essere progettato per scaricare file malevoli da Internet. Questa funzionalità è riconoscibile dall'istruzione che imposta l'URL di download nel registro EDI, seguita da un'istruzione call che chiama una funzione di download. *Dettagli Tecnici*: L'URL da cui il file malevolo viene scaricato è www[.]malwaredownload[.]com, come indicato nella Tabella 2. Il meccanismo di download è rappresentato dalla pseudo funzione DownloadToFile(), suggerendo che il malware potrebbe utilizzare una funzione personalizzata o una funzione API di sistema per scaricare il file. *Implicazioni di Sicurezza*: Il download di file da fonti esterne non verificate è un metodo di attacco comune per la consegna di payload malevoli. Questa attività può essere utilizzata per aggiornare il malware, scaricare ulteriori strumenti di hacking o installare componenti aggiuntivi malevoli.

Esecuzione di File Malevoli *Descrizione*: Il malware ha la capacità di eseguire file arbitrari presenti sul sistema infetto. Questo è evidenziato dal percorso del file Ransomware.exe specificato nel registro EDI e dal successivo utilizzo di una pseudo funzione WinExec(). *Dettagli Tecnici*: Il file specificato sembra trovarsi nel percorso C:\Program and Settings\Local User\Desktop, un percorso comune per file scaricati o creati dall'utente, rendendolo un punto di esecuzione ideale per il malware. *Implicazioni di Sicurezza*: L'esecuzione di un file, specialmente se si tratta di ransomware, può portare a conseguenze devastanti, come il criptaggio di file importanti, la richiesta di riscatto e la potenziale perdita di dati.

Analisi Approfondita La presenza di queste due funzionalità suggerisce un attacco a due fasi:

- **Fase di Distribuzione**: Il malware raggiunge la macchina vittima e stabilisce un punto d'appoggio iniziale.
- **Fase di Attacco**: Il malware procede con l'azione dannosa primaria, in questo caso, l'esecuzione di ransomware che cripta i file dell'utente.

Raccomandazioni per la Mitigazione

- **Monitoraggio del Traffico di Rete**: È essenziale monitorare tutte le connessioni di rete in uscita, soprattutto verso URL o indirizzi IP noti per essere malevoli.
- **Controllo dell'Integrità dei File**: Implementare soluzioni che monitorano l'integrità dei file sui desktop degli utenti per rilevare modifiche non autorizzate.
- **Prevenzione dell'Esecuzione di Applicazioni**: Utilizzare politiche di restrizione del software per impedire l'esecuzione di programmi non autorizzati.
- **Backup e Ripristino**: Mantenere una strategia di backup regolare e affidabile per ripristinare i dati in caso di criptaggio da ransomware.

Conclusioni Le funzionalità identificate nel malware indicano un'alta probabilità di un attacco informatico avanzato. È cruciale che gli analisti di sicurezza utilizzino queste informazioni per rinforzare le difese del sistema e preparare protocolli di risposta agli incidenti per mitigare gli attacchi e recuperare da eventuali danni. La continua vigilanza, insieme a una solida formazione degli utenti su pratiche di sicurezza informatica, è la migliore difesa contro tali minacce.

Aggiunta di Informazioni È importante notare che il malware può anche avere la capacità di nascondersi o di mascherare la sua presenza sul sistema infetto. Questo può essere fatto attraverso tecniche come il rootkitting o l'uso di funzioni di sistema per nascondere i processi in esecuzione. Inoltre, il malware può anche avere la capacità di disabilitare o interferire con il software antivirus o altre misure di sicurezza presenti sul sistema. Questo rende ancora più importante l'implementazione di misure di sicurezza robuste e l'aggiornamento regolare del software di sicurezza per proteggere il sistema da queste minacce.

Analisi delle funzionalità implementate dal Malware

Premessa:

L'esame dei segmenti di codice forniti ha permesso di rilevare alcune delle caratteristiche principali del malware in esame. Queste caratteristiche denotano un comportamento malevolo e sono comunemente utilizzate per infettare sistemi, sottrarre dati o provocare altri tipi di danneggiamenti. Caratteristiche Individuate Scaricamento di File Malevoli

- Spiegazione: Il malware sembra essere configurato per scaricare file malevoli da Internet. Questa caratteristica è riconoscibile dall'istruzione che imposta l'indirizzo del download nel registro EDI, seguita da un'istruzione call che richiama una funzione di download.
- Particolari Tecnici: L'URL da cui viene scaricato il file malevolo è www[.]malwaredownload[.]com, come indicato nella Tabella 2. Il meccanismo di download è rappresentato dalla pseudo funzione DownloadToFile(), suggerendo che il malware possa utilizzare una funzione personalizzata o una funzione API di sistema per scaricare il file.
- Conseguenze per la Sicurezza: Il download di file da fonti esterne non verificate è un metodo di attacco comune per la distribuzione di payload malevoli. Questa attività può essere utilizzata per aggiornare il

malware, scaricare ulteriori strumenti di hacking o installare componenti aggiuntivi malevoli. Esecuzione di File Malevoli

- Spiegazione: Il malware ha la capacità di eseguire file arbitrari presenti sul sistema infetto. Questo è evidenziato dal percorso del file Ransomware.exe specificato nel registro EDI e dal successivo utilizzo di una pseudo funzione WinExec().
- Particolari Tecnici: Il file specificato sembra trovarsi nel percorso C:\Program and Settings\Local User\Desktop, un percorso comune per file scaricati o creati dall'utente, rendendolo un punto di esecuzione ideale per il malware.
- Conseguenze per la Sicurezza: L'esecuzione di un file, specialmente se si tratta di ransomware, può portare a conseguenze devastanti, come il criptaggio di file importanti, la richiesta di riscatto e la potenziale perdita di dati. Approfondimento dell'Esame La presenza di queste due caratteristiche suggerisce un attacco a due fasi:
- Fase di Distribuzione: Il malware raggiunge la macchina vittima e stabilisce un punto d'appoggio iniziale.
- Fase di Attacco: Il malware procede con l'azione dannosa primaria, in questo caso, l'esecuzione di ransomware che cripta i file dell'utente. Suggerimenti per la Mitigazione
- Monitoraggio del Traffico di Rete: È fondamentale monitorare tutte le connessioni di rete in uscita, soprattutto verso URL o indirizzi IP noti per essere malevoli.
- Controllo dell'Integrità dei File: Implementare soluzioni che monitorano l'integrità dei file sui desktop degli utenti per rilevare modifiche non autorizzate.
- Prevenzione dell'Esecuzione di Applicazioni: Utilizzare politiche di restrizione del software per impedire l'esecuzione di programmi non autorizzati.
- Backup e Ripristino: Mantenere una strategia di backup regolare e affidabile per ripristinare i dati in caso di criptaggio da ransomware.

Conclusioni e mitigazione

L'indagine approfondita sulle funzionalità e sul codice del malware ci permette di comprendere le sue potenziali tattiche dannose e le strategie di attacco. L'analisi dei frammenti di codice rivela che il malware è stato progettato per eseguire azioni altamente complesse, come il download di file pericolosi e l'attivazione di payload come il ransomware, che possono infliggere danni significativi a sistemi e dati. La capacità di un malware di scaricare ed eseguire file a piacimento è particolarmente allarmante in quanto permette agli aggressori di alterare il comportamento del malware dopo l'infezione iniziale, rendendo più ardua la sua identificazione e rimozione. Questa funzionalità può essere utilizzata per mantenere un accesso persistente a un sistema compromesso, eseguire aggiornamenti del malware per eludere la rilevazione, o come parte di un attacco a più fasi. Le funzionalità rilevate richiedono una risposta di sicurezza solida e stratificata. Le organizzazioni devono adottare un approccio alla sicurezza che sia proattivo, che includa non solo la rilevazione e la mitigazione post-attacco, ma anche misure preventive. È fondamentale implementare pratiche di sicurezza complete, come l'educazione degli utenti sui potenziali vettori di attacco, la segmentazione della rete per limitare la diffusione del malware e l'adozione di soluzioni di sicurezza che sfruttano l'intelligenza artificiale e l'apprendimento automatico per identificare comportamenti anomali. Suggerimenti Finali

- Educazione e Formazione: Organizzare sessioni di formazione sulla sicurezza per gli utenti, concentrandosi sui rischi legati al download e all'esecuzione di file da fonti non verificate.

- Tattiche di Difesa Avanzate: Utilizzare strumenti di Rilevazione e Risposta degli Endpoint (EDR) e Antivirus di Nuova Generazione (NGAV) che possono identificare e bloccare comportamenti sospetti in tempo reale.
- Analisi del Comportamento: Adottare piattaforme di sicurezza che offrono analisi del comportamento e sandboxing per identificare e isolare le attività sospette prima che possano causare danni.
- Gestione delle Patch: Assicurarsi che tutti i sistemi siano sempre aggiornati con le ultime patch di sicurezza per ridurre le vulnerabilità che il malware potrebbe sfruttare. La lotta contro il malware richiede un impegno costante e una vigilanza continua. Mentre le tattiche degli aggressori si evolvono, anche le strategie di difesa devono adattarsi. La conoscenza approfondita delle capacità del malware, come quelle analizzate in questo report, è fondamentale per sviluppare una difesa efficace e per costruire un ambiente informatico più sicuro.