Analisi del Malware Win32.Mydoom.a

Introduzione

Win32.Mydoom.a è un worm di tipo mass-mailing che si è diffuso rapidamente attraverso la posta elettronica e le reti peer-to-peer (P2P). Progettato per massimizzare la sua capacità di propagazione, il malware sfrutta una struttura modulare che gli consente di eseguire una serie di azioni dannose, tra cui l'invio massivo di email infette, la raccolta di indirizzi email, l'attacco a specifici obiettivi tramite Denial of Service (DoS) e l'installazione di una backdoor per il controllo remoto.

Struttura e Funzionamento

Win32.Mydoom.a si articola in diversi moduli che collaborano tra loro per assicurare l'efficacia delle sue operazioni. Ogni modulo ha un ruolo specifico che contribuisce al comportamento complessivo del malware.

Funzionalità Principale (main.c)

Il modulo `main.c` funge da punto di ingresso principale per il malware. Questo modulo inizializza le varie componenti del worm, configurando l'ambiente di esecuzione e orchestrando le attività di propagazione e comunicazione. `Main.c` è responsabile dell'avvio delle routine di scansione del sistema, della gestione delle connessioni di rete e del controllo dei processi. Gestisce anche la creazione di thread per eseguire simultaneamente operazioni come l'invio di email, la scansione di file e la connessione ai server di comando e controllo (C2).

Generazione di Email Ingannevoli (msg.c)

Il modulo `msg.c` si occupa della creazione di email infette, con testi ingannevoli e allegati dannosi. Il malware seleziona casualmente il mittente per rendere il messaggio più credibile, spesso falsificando indirizzi legittimi. Gli allegati, mascherati da documenti o file innocui, sono in realtà eseguibili dannosi codificati in Base64 per eludere i filtri di sicurezza. Questo modulo utilizza tecniche di offuscamento ROT13 per nascondere dettagli sensibili come i domini e le estensioni dei file.

Raccolta di Indirizzi Email (scan.c)

Il modulo `scan.c` scansiona il sistema alla ricerca di file che potrebbero contenere indirizzi email, come documenti di testo, pagine web e database di posta elettronica. Questo processo consente al malware di espandere rapidamente la propria rete di

contatti, aumentando l'efficacia della sua diffusione. La scansione include anche directory temporanee di Internet e la rubrica di Outlook (WAB).

Invio delle Email Infette (xsmtp.c)

Il modulo `xsmtp.c` gestisce la connessione diretta ai server SMTP per inviare le email dannose. Questo modulo è capace di risolvere i record DNS dei server di posta e tentare ripetutamente la connessione a diversi server per massimizzare le possibilità di consegna. Inoltre, può tentare di inviare email tramite i server SMTP configurati dall'utente, migliorando la velocità di propagazione.

Creazione di Archivi ZIP (zipstore.c)

Il modulo `zipstore.c` permette al malware di creare archivi ZIP contenenti i file infetti. Questi archivi vengono poi allegati alle email per mascherare ulteriormente la natura dannosa del contenuto e superare i controlli antivirus basati su firme. L'algoritmo di compressione ZIP include la manipolazione di intestazioni e checksum CRC32 per garantire l'integrità dei file.

Attacchi Denial of Service (sco.c)

`Sco.c` è responsabile dell'esecuzione di attacchi DoS contro specifici obiettivi, come il sito www.sco.com. Il malware genera un numero elevato di richieste simultanee per sovraccaricare il server bersaglio, utilizzando tecniche di offuscamento come la cifratura ROT13 per nascondere gli indirizzi dei target nel codice sorgente. Il modulo è progettato per mantenere un attacco costante, sfruttando connessioni multiple per massimizzare l'impatto.

Funzioni di Supporto (lib.c)

Il modulo `lib.c` fornisce una serie di funzioni di supporto, tra cui la generazione di numeri casuali, la gestione delle stringhe e la conversione di dati. Inoltre, implementa algoritmi di offuscamento come il ROT13 per mascherare informazioni sensibili nel codice. Include anche funzioni per la gestione delle date SMTP, la verifica della connettività Internet e la manipolazione di file di sistema.

Comunicazione Remota (client.c)

Il modulo `client.c` consente al malware di stabilire connessioni con server remoti per il trasferimento di file eseguibili. Questo modulo è in grado di autenticarsi utilizzando specifici pacchetti di richiesta e può essere utilizzato per aggiornare o controllare il

malware da remoto. Il modulo supporta il trasferimento binario e gestisce la connessione con un meccanismo di timeout per evitare rilevamenti.

Proxy SOCKS4 (xproxy.c)

`Xproxy.c` implementa un server proxy SOCKS4 che consente agli attaccanti di utilizzare il sistema infetto come punto di accesso per ulteriori attività malevole. Il proxy supporta anche la risoluzione di nomi host e può essere sfruttato per eseguire codice dannoso ricevuto tramite la rete. Questo modulo può essere utilizzato per mascherare il traffico di rete e facilitare attività di comando e controllo (C2).

Pulizia di Eseguibili PE (cleanpe.cpp)

Il modulo `cleanpe.cpp` viene utilizzato per modificare gli eseguibili PE (Portable Executable) rimuovendo informazioni superflue e alterando i timestamp per confondere le analisi forensi. Questo modulo sovrascrive parti del codice con zeri e reimposta le intestazioni per rendere più difficile il rilevamento da parte degli strumenti di sicurezza.

Tecniche di Evasione e Persistenza

Win32.Mydoom.a utilizza diverse tecniche per evitare il rilevamento e mantenere la persistenza nel sistema infetto. Tra queste vi sono l'offuscamento del codice con ROT13, la modifica del registro di Windows per garantire l'esecuzione automatica all'avvio del sistema e l'utilizzo di thread multipli per rendere più difficile la sua rimozione. Inoltre, sfrutta il proxy SOCKS4 per comunicazioni sicure e tecniche di anti-debugging per ostacolare le analisi.

Comportamenti Malevoli

Il malware mostra una serie di comportamenti dannosi, tra cui:

- **Diffusione tramite email e P2P:** sfrutta entrambe le vie per massimizzare la diffusione.
- **Backdoor:** consente il controllo remoto del sistema infetto.
- **Attacchi DoS:** mirati a specifici siti web.
- **Furto di dati:** raccoglie indirizzi email per ulteriori campagne di spam e phishing.

- **Alterazione dei file di sistema:** modifica file eseguibili per nascondere la sua presenza.

Conclusioni

Win32.Mydoom.a rappresenta una minaccia significativa per la sicurezza informatica, grazie alla sua capacità di diffusione rapida e alle funzionalità avanzate di controllo remoto e attacco. La sua architettura modulare e le tecniche di evasione lo rendono particolarmente difficile da rilevare e rimuovere.

Raccomandazioni

Per contrastare la minaccia di Win32.Mydoom.a, è essenziale:

- **Isolare immediatamente i sistemi infetti** per prevenire ulteriori danni.
- **Effettuare un'analisi forense approfondita** per identificare eventuali compromissioni secondarie.
- **Aggiornare i software di sicurezza** e eseguire scansioni complete del sistema.
- **Monitorare il traffico di rete** per rilevare comportamenti sospetti.
- **Implementare controlli di sicurezza avanzati** per rilevare attività anomale e potenziali backdoor.

Questo report fornisce una panoramica dettagliata delle capacità e delle tecniche impiegate da Win32.Mydoom.a, offrendo le basi per una risposta efficace e tempestiva a questa minaccia.