

# Relazione Comparativa Mydoom A e B

## Comparazione tra Mydoom-A e Mydoom-B

### Funzionalità di Diffusione e Persistenza

#### 1. Mydoom-A:

- **Diffusione:** Utilizza l'invio di email infette tramite un motore SMTP interno e la rete P2P Kazaa.
- **Persistenza:** Modifica le chiavi di registro per eseguire automaticamente il malware a ogni riavvio.

#### 2. Mydoom-B:

- **Diffusione:** Mantiene l'invio di email, ma aggiunge funzioni per generare email convincenti (utilizzando vari nomi e domini) e raccoglie contatti dai file locali per migliorare la propagazione.
  - **Persistenza:** Oltre alla modifica del registro, copia se stesso nelle directory di sistema, rendendosi più difficile da rimuovere.
- 

### Backdoor e Accesso Remoto

#### 1. Mydoom-A:

- **Backdoor:** Crea una backdoor sulla porta TCP 3127 per consentire l'accesso remoto da parte degli attaccanti.

#### 2. Mydoom-B:

- **Backdoor Avanzata:** Apre una backdoor SOCKS4, stabilendo un server proxy per l'accesso remoto, permettendo esecuzione di file e controllo completo del sistema attraverso un server di comando e controllo (C&C).
-

## Offuscamento e Evasione

### 1. Mydoom-A:

- Non applica tecniche specifiche di offuscamento dei file per evitare rilevamenti.

### 2. Mydoom-B:

- **Offuscamento Avanzato:** Utilizza crittografia XOR e ROT13 e comprime i file infetti in archivi ZIP per eludere i sistemi di sicurezza.
- 

## Attacco DoS

### 1. Mydoom-A:

- **Attacco DoS:** Programmato per attaccare [www.sco.com](http://www.sco.com) a partire dal 1° febbraio 2004, sovraccaricandolo con richieste HTTP.

### 2. Mydoom-B:

- **DoS Esteso:** Migliora il DoS mirato grazie al modulo "scodos\_main" e invia traffico elevato per interrompere server specifici tramite il server C&C, aumentando l'impatto.
- 

## Funzionalità Aggiuntive in Mydoom-B


- **Decifratura e Caricamento di Librerie:** Carica una libreria di sistema (`shimgapi.dll`) per supportare l'accesso remoto.
  - **Server SOCKS4:** Permette un accesso remoto stabile per l'attaccante.
  - **Rimozione delle Intestazioni PE:** Rimuove le intestazioni superflue nei file PE per evitarne il rilevamento come malware.
-

Tabella comparativa per chiarire le principali differenze tra Mydoom-A e Mydoom-B:

Caratteristica	Mydoom-A	Mydoom-B
<b>Diffusione</b>	Invio di email infette tramite SMTP e diffusione su Kazaa (P2P).	Invio di email con nomi e domini diversi, raccolta di contatti locali, invio massivo, rete P2P.
<b>Persistenza</b>	Modifica delle chiavi di registro per avvio automatico.	Modifica delle chiavi di registro, copia nelle directory di sistema per garantire la persistenza.
<b>Backdoor</b>	Porta TCP 3127 per accesso remoto.	Backdoor avanzata con server SOCKS4 per accesso remoto e controllo tramite server C&C.
<b>Offuscamento</b>	Nessuna tecnica avanzata di offuscamento.	Crittografia XOR e ROT13, compressione dei file in ZIP per elusione di sicurezza.
<b>Attacco DoS</b>	Attacco DoS mirato su <a href="http://www.sco.com">www.sco.com</a> tramite richieste HTTP.	Attacco DoS più esteso verso server specifici con sovraccarico di traffico generato dal server C&C.
<b>Funzionalità Aggiuntive</b>	-	Decifratura e caricamento di librerie ( <code>shimgapi.dll</code> ), rimozione intestazioni PE per evitare rilevamento, server SOCKS4 per controllo remoto continuo.
<b>Misure di Prevenzione</b>	Chiusura delle porte, uso di antivirus, verifica dei backup.	Formazione utenti, utilizzo di sistemi di rilevamento avanzati (IDS), firewall, politiche di accesso limitate, backup regolari.

## Conclusioni e Rimedi

- **Mydoom-A:** Offre una base di prevenzione standard, consigliando la chiusura delle porte di rete, uso di antivirus e verifica dei backup.
  - **Mydoom-B:** Espande le misure preventive includendo formazione degli utenti e utilizzo di sistemi di rilevamento avanzato per bloccare tentativi di accesso non autorizzato.
- 

 **Chiavi Comuni:** malware, worm, mydoom, backdoor, DoS, persistenza