La versione 2.024 di MyDoom potrebbe operare nel modo seguente:

Metodi di diffusione:

La diffusione del worm avviene attraverso quattro metodi principali:

1. **Diffusione iniziale tramite hotspot falsi che simulano connessioni WiFi gratuite**.
2. **Diffusione via APK malevoli**.
3. **Diffusione tramite phishing via SMS**.
4. **Diffusione tramite phishing sui social media**.

Fase iniziale di infezione

All'inizio, il worm infetta dispositivi tramite hotspot WiFi falsi e APK malevoli. I dispositivi compromessi vengono poi indirizzati verso uno o più server di controllo, che hanno il solo scopo di mettere in comunicazione i vari dispositivi infetti. Una strategia efficace per la prima diffusione potrebbe essere simulare un WiFi pubblico in una zona molto frequentata, così da collegare i primi dispositivi alla nostra rete.

Struttura della rete peer-to-peer

I dispositivi infetti formano una rete peer-to-peer, dove ciascun nodo (dispositivo infetto) ha memorizzati gli indirizzi IP di altri dispositivi infetti a cui è collegato. Questo sistema permette di creare una rete distribuita, in cui ogni dispositivo può sia ricevere che trasmettere informazioni ad altri dispositivi nella rete, seguendo una struttura a cascata.

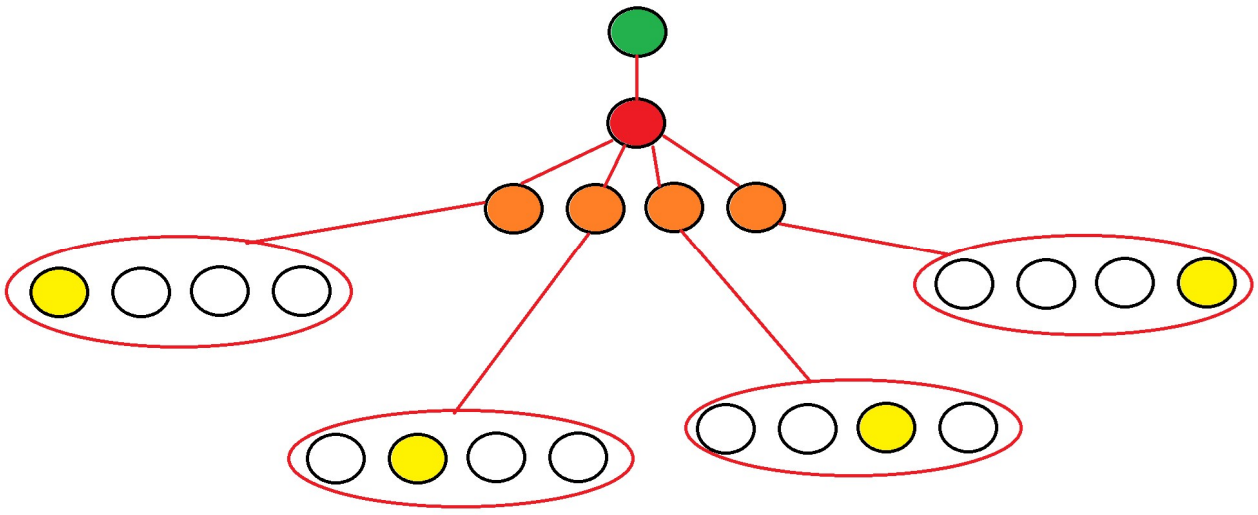
Obiettivi del worm

L'obiettivo principale del worm è ottenere l'accesso alla rubrica e agli account social media delle vittime.

- **Social media**: il worm avvia campagne di phishing direttamente dall'account della vittima, inviando messaggi apparentemente confidenziali ai contatti del proprietario.
- **Numeri telefonici**: i numeri di telefono vengono copiati e distribuiti nella rete peer-to-peer. Dispositivi infetti con la capacità di inviare SMS possono utilizzarli per avviare campagne di phishing, sfruttando il fatto che i numeri appartengono prevalentemente a utenti privati, riducendo così il rischio di incorrere in filtri anti-spam o segnalazioni.

Schema di propagazione

Il sistema di propagazione segue uno schema piramidale:



1. Un dispositivo (nodo verde) viene infettato da un altro dispositivo (nodo rosso).
2. Il nodo infettante (rosso) invia una richiesta ai nodi collegati (arancioni) per ottenere indirizzi IP di ulteriori nodi collegati (gialli), creando così un link con il nuovo dispositivo (verde).
3. In questo modo, il collegamento tra i dispositivi viene randomizzato.

Ogni nodo della rete ottiene un punteggio basato su due fattori: il tempo di attività dalla data di infezione e il numero di altri nodi già collegati. Più alto è il tempo di attività, maggiore è l'affidabilità del nodo; tuttavia, più numerosi sono i nodi collegati a un dispositivo, maggiore è il rischio di ulteriori collegamenti. Il server di controllo sfrutta questa logica per collegare i dispositivi più affidabili ai nuovi dispositivi infetti man mano che la rete si espande.

Attacco DDoS

Per lanciare un attacco DDoS non è necessario un server centrale: basta un dispositivo connesso alla rete che possa inviare un comando d'attacco. Tramite propagazione a cascata, ogni dispositivo riceve l'orario e l'indirizzo su cui lanciare l'attacco DDoS, consentendo un'azione coordinata tra tutti i nodi infetti.

In questo modo, la rete risulta immune a eventuali shutdown dei server di controllo, essendo quasi completamente decentralizzata. Ogni dispositivo infetto, anche quando in modalità dormiente, conserva gli indirizzi di altri dispositivi che possono essere attivati all'occorrenza. La diffusione iniziale tramite hotspot WiFi pubblici e APK malevoli permette inoltre di ottenere le credenziali d'accesso ai social media delle vittime, ampliando le possibilità di attacco.

A differenza della versione originale di MyDoom, per questo progetto si potrebbe adottare il protocollo SOCKS5, che offre vari vantaggi rispetto a SOCKS4:

- **Supporto per UDP**: permette comunicazioni più rapide e leggere, rendendo possibili attacchi DDoS più sofisticati.
- **Risoluzione DNS integrata**: consente di aggirare i blocchi IP, migliorando l'efficacia e la resilienza della rete infetta.
- **Compatibilità con IPv6**: aumenta la portata del malware, migliorando le possibilità di evasione e ampliando il numero di indirizzi IP a disposizione.
- **Maggiori capacità di tunneling**: SOCKS5 permette di nascondere meglio il traffico malevolo, rendendo più difficile il rilevamento da parte dei sistemi di sicurezza.

Inoltre, per rafforzare la crittografia rispetto alla versione originale di MyDoom (che utilizzava ROT13, una tecnica molto debole), si potrebbe adottare il cifrario simmetrico **ChaCha20**. Questo algoritmo offre un elevato livello di sicurezza ed è particolarmente adatto ai dispositivi mobili e a quelli con risorse limitate, grazie alle sue ottime prestazioni anche su connessioni mobili. La crittografia del payload sarebbe notevolmente più robusta, contribuendo all'evasione dei sistemi di rilevamento avanzati.