BW3 Aggiornamento Mydoom B

1. Server di Comando e Controllo (C&C) Distribuito su AWS

- **Elastic Load Balancing (ELB)**: Utilizzare un bilanciatore di carico per distribuire le richieste su diversi server C&C ospitati su AWS, rendendo la struttura più resiliente e difficile da abbattere.
- **Lambda Functions**: Usare funzioni AWS Lambda come endpoint per comunicare con le macchine infette. Lambda può eseguire codice senza richiedere un server dedicato, riducendo l'impatto visibile e i costi.
- **DynamoDB o S3 per Dati di Controllo**: Salvare comandi, aggiornamenti o liste di target in un database NoSQL come DynamoDB o in bucket S3, dove le macchine infette possono accedere in modo distribuito. DynamoDB offre query rapide e scalabilità automatica, facilitando la gestione di grandi reti infette.

2. Sfruttamento della Memoria Temporanea e Persistent Storage

- **S3 per Archiviazione Temporanea**: Salvare file o payload temporanei in bucket S3 con permessi limitati, accessibili tramite URL pre-firmati. Questo permette il recupero di file solo quando necessario, riducendo il rischio di rilevamento.
- **AWS Secrets Manager**: Conservare informazioni critiche, come chiavi di crittografia e token di accesso, in modo sicuro e accessibile alle funzioni Lambda.

3. Automatizzazione della Diffusione

- **SNS (Simple Notification Service)**: Utilizzare SNS per inviare notifiche o comandi alle macchine infette. Configurando SNS con

Lambda, le macchine infette possono ricevere aggiornamenti o comandi nuovi ogni volta che viene pubblicato un nuovo messaggio.
- **IAM Roles e Policies Restrittive**: Utilizzare ruoli IAM e policy strettamente limitate per ogni servizio AWS coinvolto, per ridurre la possibilità di rilevamento o blocco delle risorse cloud.

4. Evasione di Rilevamento

- **Utilizzo di CloudFront**: Distribuire i payload tramite Amazon CloudFront (rete CDN di AWS) per mimetizzare il traffico come traffico normale web e migliorare la latenza e disponibilità.
- **CloudWatch Logs e Metrics**: Utilizzare CloudWatch per monitorare attività e rispondere rapidamente a eventuali segnalazioni di rilevamento o problemi nella rete di distribuzione, mantenendo tutto su AWS.

5. Self-Update e Propagazione

- **Distribuzione tramite S3 e EC2 Spot Instances**: Pubblicare aggiornamenti del malware su S3 e farli scaricare periodicamente dalle macchine infette. Usare istanze Spot per caricare temporaneamente payload aggiornati senza mantenere risorse attive, riducendo i costi.
- **AWS IoT per Diffusione**: Sfruttare AWS IoT per coordinare la diffusione tra diversi dispositivi IoT connessi, che potrebbero ricevere il malware da AWS e trasmetterlo ad altri dispositivi vulnerabili nella rete.
