LOIC, acronimo di "Low Orbit Ion Cannon", è uno strumento di attacco di tipo denial-of-service (DoS) o distributed denial-of-service (DDoS). È un software open source originariamente creato per testare la sicurezza delle reti, ma è diventato noto per il suo utilizzo da parte di gruppi di hacktivisti come Anonymous per condurre attacchi contro vari siti web e servizi online.

LOIC, quando utilizzato da numerose persone contemporaneamente, effettua un attacco di tipo distributed denial-of-service (DDoS) contro un IP vittima inondando il server con pacchetti TCP, UDP o richieste HTTP, nell'intento di interrompere il servizio di un particolare host. Il funzionamento di LOIC, quindi, si basa sul contributo di volontari che, coordinandosi tra loro con altri sistemi (ad esempio: chat, forum, ecc), possono emulare una botnet.

LOIC è noto per la sua interfaccia semplice, che consente anche agli utenti meno esperti di eseguire attacchi DDoS. Gli utenti possono inserire un URL o un indirizzo IP e avviare un attacco con pochi clic.

Sebbene LOIC non offra meccanismi di anonimato intrinsechi, viene spesso utilizzato insieme a strumenti di anonimato come VPN o Tor per nascondere l'identità dell'attaccante.

Contesto Legale ed Etico

L'uso di LOIC per attacchi DoS/DDoS è illegale nella maggior parte delle giurisdizioni, in quanto costituisce un'interferenza non autorizzata con i servizi informatici. Gli attacchi possono causare danni significativi, interrompendo i servizi, causando perdite finanziarie e danneggiando la reputazione delle vittime. Pertanto, l'uso di LOIC e strumenti simili deve essere limitato a test di penetrazione e altre attività legittime con il consenso esplicito delle parti coinvolte.

Sebbene LOIC possa essere utilizzato per stress test legittimi, la maggior parte degli usi sono dannosi. Danni involontari possono derivare anche da un uso improprio da parte di utenti inesperti.

Fasi di attacco LOIC

Un tipico attacco LOIC procede attraverso diverse fasi:

1. Selezione del bersaglio

L'aggressore seleziona un sito Web, un server o una rete da interrompere. Gli obiettivi comuni sono siti aziendali, infrastrutture critiche e reti governative.

2. Armi

LOIC viene scaricato e configurato per l'attacco. Le impostazioni vengono ottimizzate, tra cui: durata dell'attacco, limiti di velocità e parametri di spoofing.

3. Lancio dell'attacco

L'aggressore lancia lo strumento LOIC contro il bersaglio. Per attacchi più grandi, vengono coordinate più istanze LOIC e botnet.

Impatto dell'attacco

Il target sperimenta la negazione del servizio, l'indisponibilità di risorse e servizi per gli utenti finali. Possono verificarsi danni finanziari, operativi e di reputazione.

4. Arresto dell'attacco

L'attacco viene fermato arrestando lo strumento LOIC. I server di backup possono essere distribuiti per ripristinare i servizi. Vengono effettuate indagini forensi per rintracciare le fonti dell'attacco.

Operation Payback

- **Data:** Settembre 2010
- **Obiettivi 1:** I primi obiettivi furono le organizzazioni anti-pirateria come la Motion Picture Association of America (MPAA) e la Recording Industry Association of America (RIAA).
- **Scopo:** Gli attacchi miravano a paralizzare i siti web di queste organizzazioni come forma di protesta contro le loro azioni legali contro la condivisione di file.
- **Obiettivi 2:** Le aziende che avevano tagliato i servizi a WikiLeaks in seguito alla pubblicazione di documenti riservati da parte dell'organizzazione, inclusi PayPal, Mastercard, Visa e Amazon.
- **Scopo:** Supportare WikiLeaks e protestare contro quello che Anonymous considerava un attacco alla libertà di informazione.