Relazione: Analisi e Mitigazione di un Potenziale Attacco Informatico

Sommario: L'analisi delle comunicazioni di rete ha rivelato segnali di compromissione (IOC) che suggeriscono un attacco in corso. Le evidenze indicano una scansione aggressiva delle porte da parte di un host sospetto.

Identificazione degli IOC: Abbiamo identificato un numero elevato di richieste TCP (SYN) dirette a porte diverse dell'host target 192.168.200.150. Queste richieste sono originate dall'host 192.168.200.100, che è stato identificato come l'attaccante.

Ipotesi sui Vettori di Attacco: Le caratteristiche dell'attività di rete osservata suggeriscono che l'attaccante sta eseguendo una scansione delle porte. Questa ipotesi è supportata dalle risposte [SYN+ACK], che indicano porte aperte, e [RST+ACK], che indicano porte chiuse, ricevute dall'host target.

Consigli per l'Azione: Per mitigare l'impatto dell'attacco, si consiglia di implementare policy firewall che bloccano l'accesso a tutte le porte da parte dell'host 192.168.200.100. Questo impedirà all'attaccante di ottenere informazioni sulle porte e i servizi in ascolto.

Dettagli Tecnici: La scansione delle porte è un metodo comune utilizzato dagli attaccanti per scoprire servizi vulnerabili. L'host 192.168.200.100 mostra un comportamento tipico di questa tecnica, inviando richieste SYN a porte casuali dell'host target e attendendo risposte.

Misure di Protezione: Si raccomanda di configurare il firewall dell'host target per respingere automaticamente tutte le connessioni in entrata dall'host sospetto. Inoltre, si dovrebbero monitorare tutte le attività di rete per identificare ulteriori tentativi di intrusione.