Relatório de incidente de segurança

Seção 1: Identifique o protocolo de rede envolvido no incidente
Os protocolos de rede primários identificados no log tcpdump foram **DNS** (para resolução de nomes de domínio) e **HTTP** (para comunicação web, incluindo solicitação de página, download de malware e redirecionamento). O **TCP** e o **IP** foram os protocolos de transporte e rede subjacentes, respectivamente, que permitiram a comunicação. O incidente focou na interação web, tornando DNS e HTTP os mais relevantes.

Seção 2: Documente o incidente
O site yummyrecipesforme.com foi comprometido por um ex-funcionário via ataque de força bruta, que explorou uma senha administrativa padrão e a ausência de controles de segurança. Após obter acesso, o invasor inseriu um JavaScript malicioso no código-fonte, que solicitava o download de um arquivo executável aos visitantes. Clientes relataram problemas após executar o arquivo, que redirecionava para greatrecipesforme.com , um site com malware. A investigação em sandbox e a análise do tcpdump confirmaram a sequência de eventos: resolução DNS para yummyrecipesforme.com , solicitação HTTP, download de malware, nova resolução DNS para greatrecipesforme.com e redirecionamento HTTP. Análises subsequentes confirmaram o script malicioso e o ataque de força bruta. **Fontes:** Relatos de clientes, observação em sandbox, log tcpdump, análise de código fonte e arquivo executável, confirmação da equipe de segurança.

Seção 3: Recomendar uma solução para ataques de força bruta
Para prevenir futuros ataques de força bruta, recomenda-se a implementação de um mecanismo para **limitar o número de tentativas de login** consecutivas. Esta medida é eficaz porque restringe o número de tentativas de senha, inviabilizando ataques automatizados. Ao bloquear temporariamente

contas ou IPs após tentativas falhas (ex:-), reduz-se a superfície de ataque, dissuade-se invasores e permite que a equipe de segurança seja alertada sobre atividades suspeitas. Isso teria impedido o acesso não autorizado no incidente atual, protegendo o site e os usuários