BOLETIM DE SEGURANÇA

Falhas permitem contorno de Firewall e DDoS na CloudFlare

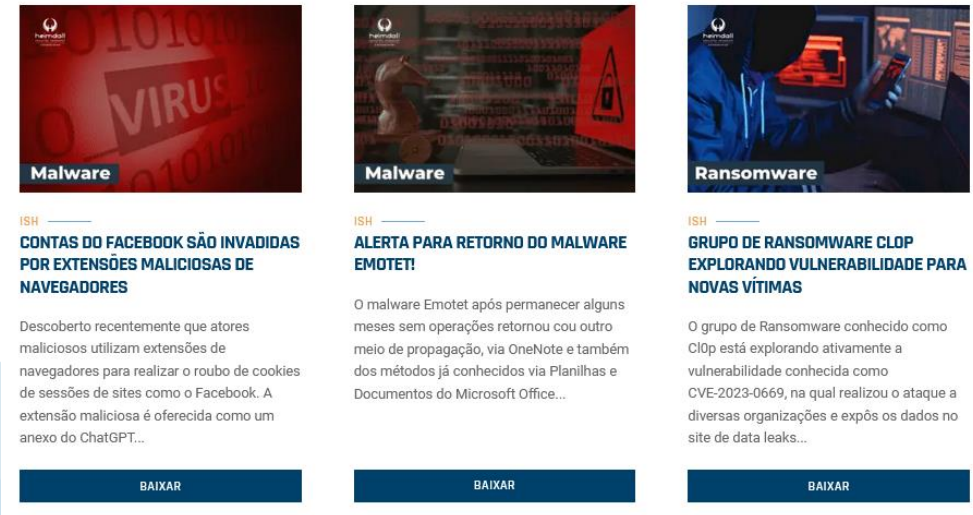
heimdall
security research
A DIVISION OF ISH

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



Sumário

Lista de Figuras

1 SOBRE AS VULNERABILIDADES CLOUDFLARE

Os serviços de proteção do **Firewall** e de **DDoS** da CloudFlare foram contornadas por meio de uma técnica que utiliza vulnerabilidades em políticas de segurança entre locatários.

O ataque requer apenas a criação de uma conta na Cloudflare gratuita pelo atacante, tornando-a facilmente acessível, porém para a exploração, os atores precisam estar cientes do endereço IP de um servidor web visado.

O uso de infraestrutura aberta pela organização que aceita conexões de todos os usuários seria a causa raiz do problema atual. A pesquisa foi divulgada pelo pesquisador Stefan Proksch. A identificou foi correlacionada a duas vulnerabilidades no sistema que afetam os **"Authenticated Origin Pulls"e o "Allowlist Cloudflare IP Addresses".**

O Authenticated Origin Pulls é um recurso de segurança fornecido pela Cloudflare para garantir que as solicitações HTTP(s) enviadas a um servidor de origem sejam provenientes da Cloudflare e não de um invasor.

Ao configurar o recurso, os clientes podem fazer upload de seus certificados usando uma API ou gerar por meio do Cloudflare.

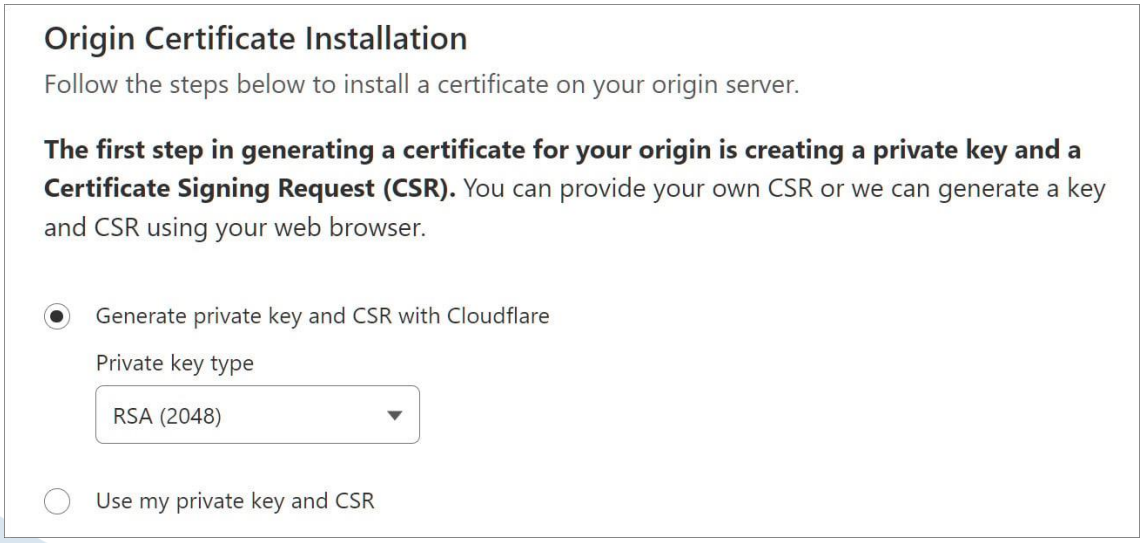


Figura 1 – Instalação do certificado de origem Cloudflare.

Depois de configurado, o Cloudfare usa o certificado SSL/TLS para autenticar quaisquer solicitações HTTP(S) entre os proxies reversos do

serviço e o servidor de origem do cliente, evitando que solicitações não autorizadas acessem o site. Porém, os invasores podem ignorar essa proteção, pois a Cloudflare usa um certificado compartilhado para todos os clientes, em vez de um certificado específico do locatário, fazendo com que todas as conexões originadas da Cloudflare sejam permitidas.

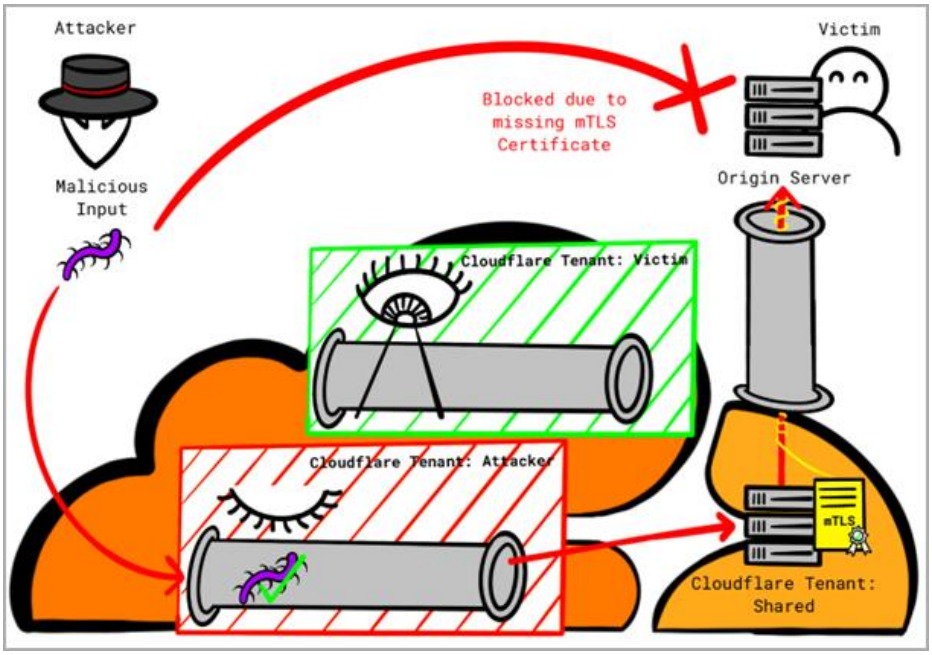


Figura 2 – Cadeia de ataque da primeira vulnerabilidade.

O problema decorrente desta lacuna é que os invasores com uma conta Cloudflare podem direcionar o tráfego malicioso para outros clientes Cloudflare ou encaminhar seus ataques através da infraestrutura da empresa.

O pesquisador afirmou que a única maneira de mitigar essa fraqueza é usar certificados personalizados em vez de certificados gerados pela Cloudflare.

Já o segundo problema, afeta os endereços IP Cloudflare da lista de permissão da Cloudflare, uma medida de segurança que permite apenas que o tráfego originado do intervalo de endereços IP da Cloudflare chegue aos servidores de origem dos clientes.

Novamente, um atacante pode aproveitar uma falha na lógica configurando um domínio com Cloudflare e apontando o registro DNS A de seu domínio para o endereço IP do servidor da vítima alvo.

Na sequência, os atacantes desativam todos os recursos de proteção de domínio personalizado e encaminham o tráfego malicioso através da infraestrutura da Cloudflare, que será vista como confiável do ponto de vista da vítima e, portanto, permitida.

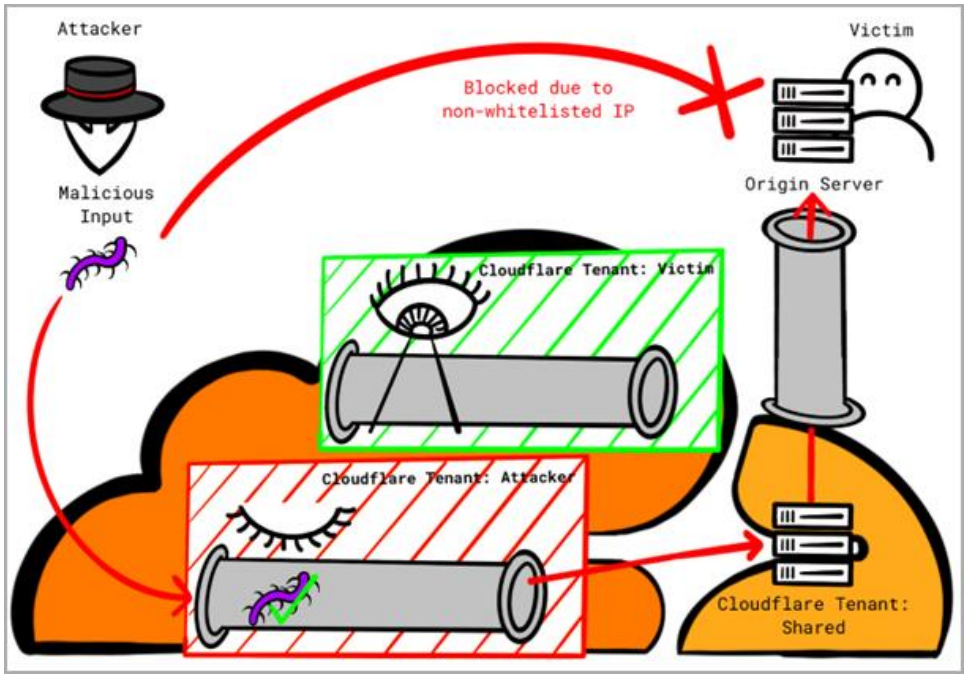


Figura 3 – Método de ataque da segunda vulnerabilidade.

O pesquisador ainda compartilhou uma PoC com detalhes de configuração para demonstrar como é fácil contornar as proteções da Cloudflare aproveitando falhas.

Portanto, para se proteger dos ataques é recomendado que:

- Utilize um certificado personalizado para configurar o mecanismo "Authenticated Origin Pulls" em vez do certificado compartilhado da Cloudflare.
- Use o Cloudflare Aegis (se disponível) para definir um intervalo de endereços IP de saída mais específico e dedicado a cada cliente.

2 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Cloudflare DDoS protections ironically bypassed using cloudflare – Bleeping Computer.**

heimdall
security research
A DIVISION OF ISH