Estudo de Caso: Invasão de Site via Força Bruta e Infecção por Malware

Resumo Executivo

Este documento detalha um incidente de segurança cibernética que afetou uma plataforma online de culinária, `yummyrecipesforme.com`. O incidente resultou no comprometimento do site, redirecionamento de usuários para uma página maliciosa e potencial infecção por malware. A investigação inicial aponta para um ataque de força bruta como vetor de acesso inicial.

Detalhes do Incidente

A plataforma `yummyrecipesforme.com`, um portal dedicado à venda de receitas e livros de culinária, foi alvo de um ataque cibernético. A investigação revelou que um ex-funcionário, motivado por insatisfação, executou um ataque de força bruta contra o host da web. Este ataque consistiu na tentativa repetida de senhas padrão conhecidas para a conta administrativa, culminando no sucesso do acesso não autorizado devido à ausência de políticas de senha robustas e controles de mitigação de força bruta.

Uma vez obtidas as credenciais de login, o invasor acessou o painel de administração do site e alterou o código-fonte. Uma função JavaScript maliciosa foi incorporada, projetada para solicitar aos visitantes o download e a execução de um arquivo ao acessarem a página principal. Após a inserção do malware, o invasor alterou a senha da conta administrativa, impedindo o acesso legítimo por parte dos administradores da plataforma.

O incidente veio à tona quando múltiplos clientes reportaram ao suporte técnico que o site havia solicitado o download de um arquivo executável para acesso a conteúdo. Após a execução do arquivo, os usuários notaram uma mudança no endereço do site em seus navegadores e uma diminuição perceptível no desempenho de seus computadores pessoais, indicando uma possível infecção por malware.

Investigação e Análise

Para compreender a dinâmica do ataque, foi simulado o comportamento do usuário em um ambiente controlado (sandbox). A análise do tráfego de rede via `tcpdump` revelou a seguinte sequência de eventos:

```
14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A?
yummyrecipesforme.com. (24)
14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A 203.0.113.22
(40)


14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [S], seq
2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859 ecr 0,nop,wscale 7],
length 0
14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: Flags [S.], seq
3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS val 3302576859 ecr
3302576859,nop,wscale 7], length 0
14:18:36.786529 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [.], ack 1,
win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 0
14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [P.], seq
1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 73:
HTTP: GET / HTTP/1.1
14:18:36.786595 IP yummyrecipesforme.com.http > your.machine.36086: Flags [.], ack 74,
win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 0
...<a lot of traffic on the port 80>...


14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A?
greatrecipesforme.com. (24)
14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A 192.0.2.17 (40)

14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags [S], seq
1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649 ecr 0,nop,wscale 7],
length 0
14:25:29.576510 IP greatrecipesforme.com.http > your.machine.56378: Flags [S.], seq
1993648018, ack 1020702884, win 65483, options [mss 65495,sackOK,TS val 3302989649 ecr
3302989649,nop,wscale 7], length 0
14:25:29.576524 IP your.machine.56378 > greatrecipesforme.com.http: Flags [.], ack 1,
win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 0
14:25:29.576590 IP your.machine.56378 > greatrecipesforme.com.http: Flags [P.], seq
1:74, ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 73:
HTTP: GET / HTTP/1.1
14:25:29.576597 IP greatrecipesforme.com.http > your.machine.56378: Flags [.], ack 74,
win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 0
...<a lot of traffic on the port 80>...
```

1. **Resolução DNS Inicial:** O navegador do usuário iniciou uma solicitação de resolução de DNS para `yummyrecipesforme.com`, recebendo o endereço IP correspondente.
2. **Solicitação HTTP:** Uma solicitação HTTP foi enviada para `yummyrecipesforme.com` para carregar a página principal.
3. **Download de Conteúdo Malicioso:** Durante o carregamento da página, o navegador iniciou o download de um arquivo executável, conforme instruído pelo código malicioso inserido.
4. **Nova Resolução DNS:** Após o download e execução do arquivo, uma nova solicitação de resolução de DNS foi observada, desta vez para `greatrecipesforme.com`.
5. **Redirecionamento HTTP:** O servidor DNS respondeu com o endereço IP de `greatrecipesforme.com`, e o navegador foi redirecionado para este novo URL, que foi identificado como a versão falsa do site contendo o malware.

Segue um documento mais detalhado de: Como ler o registro do tcpdump

Uma análise forense do código-fonte do site comprometido confirmou a adição do script JavaScript malicioso. A análise do arquivo executável baixado revelou um script responsável pelo redirecionamento dos navegadores dos visitantes. A equipe de segurança cibernética confirmou que o servidor web foi comprometido por um ataque de força bruta, facilitado pela utilização de uma senha de administrador padrão e pela ausência de mecanismos de defesa contra esse tipo de ataque.

Segue o Relatório no documento: Relatório de Incidente de Segurança