Security incident report

Section 1: Identify the network protocol involved in the incident
Protocolos de rede identificados/Identified network protocols: DNS (Domain Name System) e/and HTTP (Hypertext Transfer Protocol). Evidências dos logs do tcpdump/ Evidence from tcpdump logs: ● DNS: ○ `14:18:32.195571 IP your.machine.52444 > dns.google.domain: 35084 A? yummyrecipesforme.com. (24)` *Consulta DNS para resolver o domínio legítimo/ DNS query to resolve the legitimate domain* `yummyrecipesforme.com`. ○ `14:20:32.195571 IP your.machine.52444 > dns.google.domain: 21899 A? greatrecipesforme.com. (24)` *Consulta DNS para resolver o domínio malicioso / DNS query to resolve the malicious domain* `greatrecipesforme.com` *após o download do arquivo.* ● HTTP: ○ `14:19:36.786501 IP your.machine.36886 > yummyrecipesforme.com.http: Flags [S]...` *Início de conexão TCP (SYN) com o servidor legítimo na porta 80 (HTTP)/ TCP connection initiation (SYN) with the legitimate server on port 80 (HTTP).* ○ `14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags [S]...` *Início de conexão TCP (SYN) com o servidor malicioso na porta 80 (HTTP) após o redirecionamento/ Initiating a TCP (SYN) connection with the malicious server on port 80 (HTTP) after redirection..* Conclusão/ Conclusion: Os protocolos DNS (para resolução de domínios) e HTTP (para transferência de dados) foram explorados para redirecionar usuários do site legítimo (`yummyrecipesforme.com`) para o site malicioso (`greatrecipesforme.com`). The DNS (for domain resolution) and HTTP (for data transfer) protocols were exploited to redirect users from the legitimate website (yummyrecipesforme.com) to the malicious website (greatrecipesforme.com).

Section 2: Document the incident

Resumo detalhado do incidente:
Em 10 de setembro de 2025, o site `yummyrecipesforme.com` foi comprometido por um ex-funcionário que realizou um ataque de força bruta contra a conta administrativa. O invasor explorou o uso de uma senha padrão no painel de administração, gaining acesso ao código-fonte do site. Um script JavaScript malicioso foi inserido, o qual solicitava que os visitantes baixassem e executassem um arquivo disfarçado como "atualização de navegador".

Após a execução do arquivo, os navegadores dos usuários foram redirecionados para `greatrecipesforme.com` (IP: `192.0.2.17`), que hospedava malware. Vários clientes relataram lentidão em seus dispositivos e mudanças no comportamento do navegador.

Fontes de evidência:

- Logs do tcpdump: Mostram o tráfego DNS e HTTP, incluindo o redirecionamento de `yummyrecipesforme.com` (IP: `203.0.113.22`) para `greatrecipesforme.com` (IP: `192.0.2.17`).
- Análise do código-fonte: Confirmou a inserção de JavaScript malicioso no site legítimo.
- Relatos de clientes: E-mails ao helpdesk queixando-se de solicitação de download suspeita e redirecionamento.
- Tentativa falha de login: O proprietário não conseguiu acessar o painel administrativo devido à alteração da senha pelo invasor.

Impacto:

- Usuários expostos a malware após download e execução do arquivo.
- Comprometimento da confiança na marca e possíveis danos financeiros;

Detailed Incident Summary:

On September 10, 2025, the website yummyrecipesforme.com was compromised by a former employee who performed a brute-force attack against the administrative account. The attacker exploited a default password in the admin panel, gaining access to the website's source code. A malicious JavaScript script was inserted, prompting visitors to download and run a file disguised as a "browser update."

After executing the file, users' browsers were redirected to greatrecipesforme.com (IP: 192.0.2.17), which hosted malware. Several customers reported slowdowns on their devices and changes in browser behavior. Evidence Sources:

tcpdump logs: Show DNS and HTTP traffic, including the redirection from

yummyrecipesforme.com (IP: 203.0.113.22) to greatrecipesforme.com (IP: 192.0.2.17).

Source Code Analysis: Confirmed the insertion of malicious JavaScript into the legitimate website.

Customer Reports: Emails to the helpdesk complaining about a suspicious download request and redirection.

Failed Login Attempt: The owner was unable to access the admin panel due to the attacker changing the password.

Impact:

Users exposed to malware after downloading and executing the file.

Brand trust compromised and potential financial damages.

Section 3: Recommend one remediation for brute force attacks

Medida de segurança recomendada:
Implementar autenticação de dois fatores (2FA) para todas as contas administrativas.

Justificativa:

- A 2FA exige um segundo fator de autenticação (ex.: código via aplicativo móvel ou SMS) além da senha, impedindo que invasores acessem contas mesmo que obtenham credenciais através de força bruta.
- É uma prática recomendada pelo NIST e amplamente adotada para proteger contas privilegiadas.
- Reduz significativamente o risco de acesso não autorizado, complementando outras medidas como senhas fortes e limite de tentativas de login.

Ações adicionais sugeridas:

- Eliminar o uso de senhas padrão em todos os sistemas.
- Implementar bloqueio de conta após múltiplas tentativas falhas de login.
- Auditar regularmente as contas administrativas e suas permissões.

Recommended security measure:
Implement two-factor authentication (2FA) for all administrative accounts.

Rationale:

- 2FA requires a second authentication factor (e.g., a code via mobile app or SMS) in addition to the password, preventing attackers from accessing accounts even if they obtain credentials through brute force.
- It is a practice recommended by NIST and widely adopted to protect privileged accounts.
- It significantly reduces the risk of unauthorized access, complementing other measures such as strong passwords and limiting login attempts.

Additional suggested actions:

- Eliminate the use of default passwords across all systems.
- Implement account lockout after multiple failed login attempts.
- Regularly audit administrative accounts and their permissions.