Security incident report

Section 1: Identify the network protocol involved in the incident
Protocolos envolvidos no acidente, e como eles aconteceram: IP: Protocolo responsável por transportar os pacotes entre origem e destino. No caso, encapsula a consulta DNS (via UDP) e a conexão HTTP (via TCP). UDP: Sendo feita usando DNS, para requisição do IP do site via DNS, usado por padrão na porta 53. DNS: Protocolo que solicita ao servidor DNS o endereço IP associado a um domínio (ex.: `yummyrecipesforme.com` e `greatrecipesforme.com`). TCP: Usado para garantir a entrega confiável dos dados HTTP, com handshake de três vias, e depois rodando o HTTP. HTTP: Indica uma página na web, no caso ali ele estava fazendo alusão a porta web 80; SYN: Flag de sincronização do cliente/servidor; ACK: Flag de confirmação do servidor/cliente; OBS: Podendo notar que antes e depois que temos linhas igual como: [S]: início da conexão->   [S.] confirmação do ínicio da conexão pelo servidor (SYN/ACK)->   [.]cliente confirma o recebimento da resposta(ACK) | [P.]Envio de dados +confirmação (ACK) ->   [.] uma confirmação do recebimento de dados (ACK) pelo cliente.   Mesmo que o domínio resolva para o IP malicioso, o cliente executa processo de handshake e transmissão de dados, pois o TCP não valida a legitimidade.

Section 2: Document the incident

```
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)
```

Nesse primeiro trecho do log, nota-se que o cliente tenta acessar o dominio yummyrecipesforme.com, onde é feita uma consulta UDP na porta 53, usando o protocolo DNS, perguntando, qual o ip desse domínio? Assim o servidor DNS devolvendo o IP associado ao domínio, vindo em uma resposta encapsulada em um pacote UDP/IP até o cliente.

```
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>...
```

1 a 3 linha:
Origem: your.machine porta:36086
destino:yummyrecipesforme.com porta:80(HTTP)
Flag:[S] sincronização com o servidor(SYN)
Length 0:Ainda não há dados, só sincronização.

4 a 6 linha:
Origem :yummyrecipesforme.com porta:80(HTTP)
Destino:your.machine porta:36086
Flag: [S.] Pedido de sincronização confirmado pelo servidor(SYN/ACK)
OBS:Basicamente um handshake padrão para a entrada no dominio

7 a 9 linha:
Origem: your.machine porta:36086

destino:yummyrecipesforme.com porta:80(HTTP)
Flag:[.] Cliente confirma recebimento de confirmação de suincronização(ack)
Obs:Só um handshake padrão, dando para notar a diferença do destino e origem.

10 a 12 linha:
Origem: your.machine porta:36086
destino:yummyrecipesforme.com porta:80(HTTP)
Flag:[P.] Envio de dado + confirmação de sincronização(ACK)
Length 73: HTTP: GET / HTTP 1.1 -> pedindo a página principal
Cliente está enviando um pacote TCP com requisição HTTP GET/ HTTP/1.1
Basicamente ele está dizendo para abrir a página principal do site.

13 a 15 linha:
Origem :yummyrecipesforme.com porta:80(HTTP)
Destino:your.machine porta:36086
Flag: [.] Confirmação de recebimento de dados pelo cliente(ACK)
Término e abertura do site

```
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>...
```

Para um resumo mais centralizado, nota-se que ao acessar o domínio malicioso, ele entra normalmente, fazendo todas as etapas de handshake e transmissão de dados até a abertura. Fazendo exatamente igual ao site

real(yummyrecipesforme.com), mesmo caminho de flags, mesmo acesso a porta HTTP, só que a única coisa que muda é na hora da requisição que o servidor DNS faz, aonde ele traz outro IP de domínio, onde traz o IP errado para abertura do sistema web.
Caso real:

Já sabendo que os invasores conseguiram acesso ao servidor por meio de um brute force simple(tentativa e erro em senhas)e colocaram um arquivo JS, que quando acontece a tentativa de entrar no domínio ele baixa um arquivo, e depois faz outra solicitação DNS ao servidor, só que agora informando o endereço de IP do site falso.

Caso adverso:
OBS: Podemos citar que esse ataque talvez aconteceu por um DNS SPOOFING, que consiste em alterar a resposta do DNS para que um domínio legítimo seja resolvido para um endereço IP malicioso. Fazendo que o usuário seja redirecionado a um domínio cópia, sendo muito mais fácil o roubo de dados organizacionais/pessoais.

Conclusão:
Pode-se ter várias conclusões nessa questão, mas a mais provável seria realmente de um DNS Spoofing, onde no momento em que o servidor DNS responde a consulta do cliente, um agente malicioso tenha interceptado ou modificado essa resposta, fazendo com que o DNS retorna um endereço IP falso - o IP, do servidor controlado por ele. Assim, o cliente é direcionado para uma cópia falsa do site original, sem saber o que estava acessando realmente.

Section 3: Recommend one remediation for brute force attacks
Soluções: Servidor/senhas: Reformulação de políticas de senhas em todas as empresas, pois se os invasores conseguiram invadir o servidor com brute force simples, é por que a política está fraca. Dica:Criação de regras para +8 caracteres(letras ou números),2 caracteres especiais, não pode ser algo igual as últimas 3 últimas senhas, nada que tenha alusão ao seu nome ou data de nascimento. Também travando login, com tentativas até 4 erros no login, trazendo um aviso ao ADMIN.

Autenticação de 2 fatores MFA, se é em um servidor, conversar com o pessoal do sistema do servidores, ou o próprio pessoal do TI, ver de alguma forma obter uma dupla autenticação, tanto para controle de pessoas que entram em saem do servidor.

Conscientização social:
Investir em treinamentos mensais sobre cibersegurança para funcionários, pois desse jeito eles vão saber a ler URLs, endereço de email, email malicioso, engenharia social maliciosa, etc.

Situação adversa:

Manter o sistema e softwares sempre atualizados, maioria dos ataques são de sistemas mal atualizados.

Usar DNS seguro e confivale como Google DNS (8.8.8.8 / 8.8.4.4), cloudflare(1.1.1.1), etc

Use DNS sobre HTTPS (DoS) OU dns sobre TLS (DoT), protocolos que criptografam as consultas DNS, impedindos que atacantes na rede interceptam e modifiquem as respostas DNS.