English:

Security incident report

Section 1: Identify the network protocol involved in the incident
Basically, the incident was caused by a vulnerability in the website's addressing, which caused the problem that when accessing the website “yummyrecipesforme.com” it was redirected to another website with a malicious file called “greatrecipesforme.com”, both using the Hypertext Transfer Protocol (HTTP). This is clearly a brute force attack with a bit of social engineering, making customers think they are on the right website, but using a deceptive website.

Section 2: Document the incident
After receiving feedback from several customers, we noticed the incident and investigated what might be happening, claiming that they were asked to download and execute files to continue access. However, first of all, I would like to give a preliminary explanation about the Hypertext Transfer Protocol (HTTP): “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)” Analyzing the “tpdump” we see that this would be the correct operation of the site, requesting the DNS of the Google domain, and redirecting us to the correct server hosted by the site, with “203.0.113.22” being the IP of “yummyrecipesforme.com”. After that, it registers the connection to the site, re14:18:36.786501 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
```

As we can see, the traffic request from the website seems normal, where it requests the port connection and is destined. But...

```
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
```

Here we notice something different, where here it seems that it is the moment that is the request for the download of the malware, at the moment, using the "...HTTP: GET / HTTP/1.1." showing that the browser is requesting data from the website.

```
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 192.0.2.172 (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
```

And at that moment it completely changes the traffic logs, starting to route again on a source computer DNS port 52444, the Google domain "IP your.machine.52444 > dns.google.domain:" and this time going to an IP (192.0.2.172) an IP associated with "greatrecipesforme.com" and changing the route precisely to the website hosted by the criminal.

Section 3: Recommend one remediation for brute force attacks
I believe that good security practices in the company would be important, such as prohibiting the use of old passwords for registration, requesting regular password changes, strong passwords with special characters and numbers, MFAs, two-factor authentication. On the part of the company, it would be interesting to have a monitoring of login controls and limit login attempts. I believe these would be good practices to avoid possible attacks similar to this one and also possible attacks on the network infrastructure, such as DDoS and SYN attacks.

Português:

Relatório de incidente de segurança

Seção 1: Identifique o protocolo de rede envolvido no incidente
Basicamente o incidente foi feito por uma vulnerabilidade de

endereçamento do site, fazendo com que o problema quando acessar o site "**yummyrecipesforme.com** " era encaminhado para outro site com arquivo malicioso chamado "**greatrecipesforme.com**" sendo ambos no protocolo Hypertext Transfer Prototol (HTTP).

Esse sendo claramente um ataque usando brute force com um pouco de engenharia social, fazendo com que clientes pensem que estão no site certo, mas utilizando um site enganoso.

Seção 2: Documente o incidente

Após o feedback de diversos clientes notamos o incidente, e fomos investigar o que pode está acontecendo,alegando que foram solicitados a baixar e executar arquivos para continuar o acesso, mas antes de tudo gostaria de dá uma preve explicação sobre o Hypertext Transfer Prototol (HTTP):

"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)"

Analisando o "tpdump" vemos que essa seria a operação correta do site, solicitando o DNS do domínio do google, e nos redirecionando para o servidor correto hospedado pelo site, sendo "203.0.113.22" o IP do "yummyrecipesforme.com". Após isso registra a conexão do site, solicitando a porta de destino 36086 indo para o site:

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

Como vemos a solicitação do trafego do site parece normal, onde ele solicita a conexão da porta e é destinado. Mas...

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
```

Aqui notamos algo diferente, onde aqui parece que é o momento que é a solicitação para o download do malware, no momento, usando o "...**HTTP: GET / HTTP/1.1.**" mostrando que o navegador está solicitando dados 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 192.0.2.172 (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
```

E nesse momento muda completamente os logs do tráfego, passando a rotear novamente em um computador de origem DNS de porta 52444, o domínio do google "`IP` **your.machine.52444 > dns.google.domain:**" e dessa vez indo para um ip (192.0.2.172) um ip associado a "**greatrecipesforme.com**" e mudando a rota justamente o site hospedado pelo criminoso**.**

Seção 3: Recomende uma correção para ataques de força bruta
Acredito que boas maneiras de segurança na empresa seriam importantes, como proibir o uso de senhas antigas para registro, a solicitação de mudança de senha regularmente, senhas fortes com caracteres especiais e números, MFA's ,autenticação de dois fatores, por parte da empresa seria interessante ter uma monitoria de controles de login e limitar as tentativas de fazer login.

Acredito essas seriam boas práticas para evitar possíveis ataques parecidos como esse e também possíveis ataques na infraestrutura da rede, como DDoS e SYN attack.