GLEN TABERIMA

Cybersecurity Incident Report: BruteForce Attack

Exploiting HTTP Protocol on Website

Identify the network protocol involved in the incident
Protokol yang terkena dampak dalam insiden tersebut adalah Hypertext Transfer Protocol (HTTP). Menjalankan tcpdump dan mengakses situs yummyrecipesforme.com untuk mendeteksi masalah, menangkap protokol, dan aktivitas lalu lintas dalam file log. Traffic DNS & HTTP memberikan bukti yang diperlukan untuk sampai pada kesimpulan ini. File berbahaya diamati sedang diangkut ke komputer pengguna menggunakan protokol HTTP di application layer.

Document the incident
Beberapa pelanggan telah menghubungi pemilik situs web dan melaporkan bahwa ketika mereka mengakses situs tersebut, mereka diminta untuk mengunduh dan menjalankan file yang mengklaim untuk melakukan pembaruan pada peramban web mereka. Setelah mengunduh file tersebut, kinerja komputer pribadi mereka menjadi lambat. Pemilik situs web mencoba masuk ke server web, namun menyadari bahwa akunnya telah terkunci. Tim analis keamanan siber menggunakan sandbox untuk menguji situs web tanpa merusak jaringan perusahaan. Selanjutnya, analis menjalankan tcpdump untuk merekam paket data dan protokol yang dihasilkan selama interaksi dengan situs web tersebut. Analis juga diminta untuk mengunduh dan menjalankan file yang diklaim sebagai pembaruan peramban, yang mengarahkan mereka ke situs web palsu (greatrecipesforme.com) dengan tampilan yang mirip dengan situs aslinya (yummyrecipesforme.com). Setelah memeriksa log tcpdump, analis mengamati bahwa peramban awalnya meminta alamat IP untuk situs yummyrecipesforme.com. Setelah koneksi HTTP ke situs tersebut terjadi, analis menemukan perubahan tiba-tiba dalam lalu lintas jaringan saat peramban meminta resolusi IP baru untuk URL greatrecipesforme.com. Lalu lintas jaringan kemudian dialihkan ke alamat IP baru untuk situs web greatrecipesforme.com. Seorang profesional keamanan siber senior menganalisis kode sumber situs web dan file yang diunduh. Analis menemukan bahwa penyerang telah memanipulasi situs web dengan menambahkan kode yang mendorong pengguna untuk mengunduh file berbahaya yang menyamar sebagai pembaruan peramban. Karena pemilik situs web

menyatakan bahwa akun administrator telah dikunci, analis yakin bahwa penyerang menggunakan serangan brute force untuk mengakses akun dan mengubah kata sandi admin. Eksekusi file berbahaya tersebut mengancam keamanan komputer pengguna akhir.

Sebelumnya, pengujung melaporkan bahwa setelah mengakses situs yummy, browser melakukan pengunduhan file dan setelah file diinstal, website akan diarahkan ke nama situs yang lain dengan produk yang dijual secara gratis.
Kejadian terjadi pada:
14:18:32 terjadi permintaan resolusi DNS dari port 52444 ke DNS server dns.google.domain untuk tujuan website yummyrecipt dan dns membalas IP yg benar milik website asli.

Jam 14:18:36, permintaan koneksi Dari port 36086 ke port 80 dan koneksi diterima oleh webserver. Kemudian browser meminta data pada website yummy melalui metode GET HTTP protokol versi 1.1 dan terjadi pengunduhan file.

Jam 14:20-38, melalui port 56378 browser melakukan permintaan resolusi DNS ke alamat website dan IP baru serta memulai http request ke website yang baru.

Recommend one remediation for brute force attacks
Salah satu langkah keamanan yang akan diterapkan oleh tim untuk melindungi dari serangan brute force adalah otentikasi dua faktor (2FA). Paket 2FA ini akan mencakup persyaratan tambahan bagi pengguna untuk memvalidasi identifikasi mereka dengan mengkonfirmasi kata sandi satu kali (OTP) yang dikirimkan ke email atau telepon mereka. Setelah pengguna mengonfirmasi identitas mereka melalui kredensial login dan OTP, mereka akan mendapatkan akses ke sistem. Aktor jahat mana pun yang mencoba melakukan serangan brute force kemungkinan besar tidak akan mendapatkan akses ke sistem karena memerlukan otorisasi tambahan.

Melakukan pergantian kata sandi default menjadi kata sandi yang baru serta menerapkan password kuat dengan kriteria, memiliki panjang lebih dari 10 karakter, uppercase, lowercase, spesial karakter

DNS & HTTP Traffic Log

```
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>...
```