03. Brute Force Saldırısı ve Çözümleri

```
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)
```

```
14:20:32.192571 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)
```

Bölüm 1: Bu olaya dahil olan network protokolü hangisidir?

HTTP protokolü söz konusudur. Söz konusu sorun şirketin website'sine (yummyrecipesforme.com) bağlanmaya çalışırken gerçekleşiyor ve bildiğimiz üzere HTTP bundan sorumlu olan protokoldür.

Bölüm 2: Sorunu raporlayın

Bazı kullanıcılar firmanın internet sitesi yummyrecipesforme.com'a bağlanmaya çalışırken bir sorunla karşılaştıklarını bildirdi. Bağlanmaya çalışırken tamamen farklı olan başka bir web sitesine (greatrecipesforme.com) yönlendirildiklerinii bildirdiler. Yönlendirildikten sonra bilgisayarları bir dosya indirmeye başladı ve o zamandan beri bilgisayarları yavaş durumda Ayrıca hesaplarına erişimlerini kaybettiler. Siber güvenlik analistleri sorun gidermek için tcpdump'ı kullandı. Kısa süre sonra saldırganların güncelleme indirme kodunu değiştirdiği ve bunun yerine zararlı bir kötü amaçlı yazılım yerleştirdiği anlaşıldı. Ayrıca saldırganlar, hesaplarının tam kontrolünü ele geçirmek için kullanıcıların şifrelerini de değiştirmişti.

Bölüm 3: Brute Force saldırısına çözüm sunun

Brute Force saldırısını sorun olmaktan çıkarmanın en iyi yolu MFA (Çok Faktörlü Kimlik Doğrulama) kullanmaktır. Ayrıca kullanıcıların 6 ayda bir sürekli olarak şifrelerini değiştirmeleri zorunlu olmalıdır. Bir şifreyi uzun süre kullanmak, hacker'ların şirketteki birisinin şifresini tahmin ederek erişim elde etmesine ya da çalınma olasılığını arttırmasına yardım etmekten başka bir işe yaramayacaktır.