APT Saldırısı Nedir?

APT, yani Advanced Persisten Threat hedefin belli olduğu, saldırganın motivasyonunun uzun soluklu olduğu, kullanılan yöntemlerin detaylı aşamalardan oluştuğu ve yönteme göre tool'ların geliştirildiği saldırı türüne verilen addır. Stuxnet APT saldırılarına verilebilecek en güncel örnektir.

Hatırlarsanız sızma testlerinde kabul görmüş ve uygulanan methodoloji aşağıdaki adımlardan oluşmaktaydı:

- Bilgi Toplama
- Zayıflık Tarama
- Sisteme Sızma
- Kalıcı Olma
- İzleri Temizleme
- Raporlama

Ancak son zamanlarda saldırganlar teknik olarak bilgili ve becerikli olmakla beraber hedef kurum personeliyle doğrudan iletişim kurabilecek tekniklere de sahip olduklarından sıradan saldırganların yöntemlerine dayanarak hazırlanan ve sektör genelinde kullanılan sızma testleri methodolojisi yetersiz kalmaktadır. Dolayısıyla Sızma Testleri dışında APT Değerlendirme Testlerine de ihtiyaç vardır.

NOT: BGA tarafından gerçekleştirilen APT testlerinde internet üzerinden teste tabi tutulan bir kurumdan herhangi bir bilgi almadan o kuruma sızma başarı oranı %100'dür.

Kaynak

https://www.bgasecurity.com/danismanlik-hizmetleri/sosyal-muhendislik-testleri/