**4. ScareCrow – AMSI ve ETW Bypass ile Payload Çalıştırıcı**

**Nedir?**

ScareCrow, modern Windows sistemlerinde çalışan, AMSI (Antimalware Scan Interface) ve ETW (Event Tracing for Windows) gibi güvenlik önlemlerini atlatmak amacıyla tasarlanmış bir payload loader (yükleyici) aracıdır. Bu araç, özellikle shellcode'ların sessiz ve fark edilmeden çalıştırılması için geliştirilmiştir.

**Özellikleri:**

✓AMSI Bypass: Antivirüs yazılımlarının script analizine müdahalesini engeller.

✓ETW Patchleme: Davranış izleme sistemlerinden kaçmayı sağlar.

✓SysWhispers2 desteği ile Native API çağrılarını gizli şekilde kullanır.

✓Go diliyle yazılmıştır – taşınabilir ve hızlıdır.

✓Payload’ı EXE veya DLL formatında üretme imkanı sunar.

✓Komut satırı üzerinden özelleştirilebilir üretim.

**Kullanım Alanları:**

✓AV/EDR sistemlerinden kaçınarak zararlı kodu çalıştırmak

✓Red Team operasyonlarında "stealth" (gizlilik) odaklı saldırılar

✓PowerShell gibi araçlara karşı alınan modern güvenlik önlemlerini devre dışı bırakmak

✓Eğitim ortamlarında AMSI/ETW mimarisini test etmek

**Kurulum Aşamaları:**

**- Gereksinimler:**

•Go dili (GoLang)

•Windows için Mingw-w64 (derleyici)

•Git

**- Adımlar**:

**1**. Kod deposunu klonlayın: 

**2.** Go bağımlılıklarını yükleyin: 

**3**. Payload oluşturun: 

**4**. İstenilen formatta EXE ya da DLL çıktısı alabilirsiniz.

**Dikkat Edilmesi Gerekenler:**

✓Gerçek sistemlere uygulanması yasal değildir; yalnızca izinli test ortamlarında kullanılmalıdır.

✓Payload şifrelenmemişse bazı AV sistemleri yine de tespit edebilir.

✓ETW patch’leri bazı sistemlerde olay kaydı eksikliğine yol açabilir.

✓Go dili ile derlenen dosyalar bazı sistemlerde büyük boyutlu olabilir.