**Badger Nedir?**

**Badger**, gelişmiş bir **post-exploitation** (istismar sonrası) aracı ve shellcode loader’dır. Windows işletim sistemlerinde çalışacak şekilde tasarlanmış olan Badger, hafif ve sezilmesi zor yapısıyla, antivirüs ve EDR çözümlerinden kaçınmak amacıyla oluşturulmuştur.

Badger, arka kapı bağlantıları (backdoor) ve uzaktan komut yürütme (remote execution) gibi işlemleri gizlice gerçekleştirebilir. Genellikle **Cobalt Strike, Mythic veya Sliver gibi C2 (Command and Control) sistemleri** ile entegre çalışır.

**Temel Özellikleri**

1. **Shellcode Loader (Yükleyici):**
   * Windows sistemlere shellcode enjekte ederek uzaktan komut çalıştırılmasını sağlar.
   * Assembly, C, ve C++ ile uyumlu şekilde tasarlanmıştır.
2. **EDR/AV Atlama (Evasion):**
   * Antivirüs yazılımlarından kaçmak için özel teknikler (örneğin: inline hooking atlama, DLL injection, syscalls) kullanır.
   * Hedef sistemde daha uzun süre fark edilmeden kalabilir.
3. **Dinamik Payload Desteği:**
   * AES şifrelenmiş payload’lar kullanarak ağda fark edilmeden iletişim kurabilir.
4. **Memory Injection:**
   * Hedefte çalışan bir işlemin hafızasına doğrudan zararlı kod enjekte edebilir.
5. **Çok Katmanlı İletişim (C2):**
   * HTTP, HTTPS, DNS ve hatta custom protokoller üzerinden komut kontrolü destekler.
6. **Modüler Yapı:**
   * Kullanıcının ihtiyacına göre özelleştirilebilecek şekilde tasarlanmıştır.
   * Yükleme sırasında hangi modülün kullanılacağı seçilebilir.

**Hangi Alanlarda Kullanılır?**

1. **Red Team Operasyonları:**
   * Kurum içi güvenlik önlemlerinin ne kadar etkili olduğunu ölçmek için, kırmızı takım tarafından saldırı simülasyonlarında kullanılır.
2. **Post-Exploitation / Erişim Sonrası Aşama:**
   * Başarılı bir sızma sonrası, sistemde derinlemesine kontrol elde etmek için kullanılır.
   * Sistem üzerinde kalıcılık, veri toplama, daha fazla yayılma (lateral movement) gibi adımların gerçekleştirilmesini sağlar.
3. **EDR Bypass Testleri:**
   * Güvenlik sistemlerinin ne kadar tespit yeteneğine sahip olduğunu test etmek için kullanılır.

**⚠️ Yasal Uyarı**

Badger gibi araçlar **çok güçlü ve tehlikeli** olabilir. Sadece aşağıdaki şartlarda kullanılması etik ve yasaldır:

* Hedef sistem sahibi tarafından **açık yazılı izin** verilmişse
* **Eğitim veya laboratuvar ortamlarında** test ediliyorsa
* **Adli analiz veya güvenlik danışmanlığı** çerçevesinde kullanılıyorsa

İzinsiz kullanımı, **TCK (Türk Ceza Kanunu)** ve diğer ülkelerdeki siber suç yasaları gereği **ağır suç** teşkil eder.



**💼 Ek Özellikler ve Kullanım Notları**

* **AES Key Rotation:** Her oturumda farklı şifreleme anahtarı kullanarak iletişimi daha güvenli hale getirir.
* **Syscall Obfuscation:** Windows API çağrılarını gizleyerek antivirüslerin tespitini zorlaştırır.
* **Custom Loader Geliştirme:** Kendi C2 sisteminle iletişim kuracak özel modüller yazılabilir.

**🧠 Sonuç**

**Badger**, gelişmiş sızma testleri ve istismar sonrası analiz için son derece güçlü bir araçtır. Özellikle antivirüs atlatma (AV evasion) ve kalıcılık (persistence) konularında başarı sağlar. Ancak bu kadar güçlü bir aracın kullanımı ciddi etik ve yasal sorumluluklar doğurur.

Eğitim, farkındalık ve kurum içi denetimler için kullanımı, bilgi güvenliği ekiplerinin savunmalarını daha etkin hale getirmesine yardımcı olur. Ancak izinsiz kullanım, ağır cezai sonuçlar doğurabileceğinden **mutlaka etik sınırlar içinde kalınmalıdır**.