QuasarRAT Aracı - Eğitim Materyali

# 🧠 QuasarRAT Nedir?

QuasarRAT, açık kaynaklı, Windows tabanlı bir Uzaktan Erişim Truva Atı (Remote Access Trojan - RAT) aracıdır. Red Team senaryolarında ve siber güvenlik laboratuvarlarında uzaktan kontrol, bilgi toplama ve sistem manipülasyonu gibi işlemleri gerçekleştirmek için kullanılır. Hafif, hızlı ve C# ile yazılmıştır.

# 🚀 Özellikleri

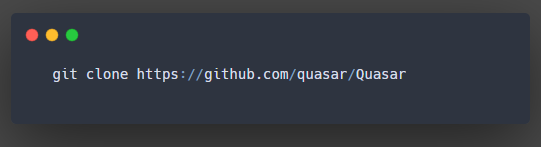
- Uzaktan masaüstü (Remote Desktop) erişimi  
- Dosya yönetimi (upload/download/delete)  
- Keylogger (tuş kaydedici)  
- Komut satırı/PowerShell çalıştırma  
- Web kamerası ve mikrofon erişimi  
- Şifre çalma ve sistem bilgisi toplama

# 🎯 Kullanım Alanları

- Red Team uzaktan kontrol senaryoları  
- İç ağ testleri ve kullanıcı etkileşimi testleri  
- Siber güvenlik eğitimleri ve simülasyon ortamları  
- Malware analiz laboratuvarlarında zararlı yazılım eğitimi

# 🛠️ Kurulum ve Yapılandırma

1. GitHub üzerinden QuasarRAT indirilir:

******

2. Visual Studio ile açılır ve build edilir (.exe dosyası oluşur).

3. Sunucu tarafında Quasar.exe çalıştırılır.

4. 'Builder' arayüzünden istemci oluşturulur (IP, port, şifre belirlenir).

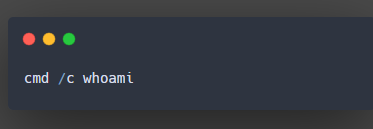
5. Oluşan istemci hedef sisteme gönderilir ve çalıştırılır.

# 🧪 Örnek İşlemler

✅ Bağlantı Kurulunca Sunucuda Görünenler:

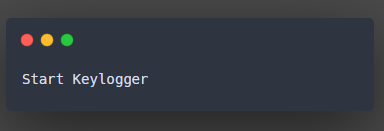
- IP Adresi  
- Kullanıcı adı  
- İşletim sistemi bilgisi  
- Bağlantı süresi

✅ Uzaktan Komut Çalıştırma:

******

→ Hedefte kim oturum açmış, gösterir.

✅ Keylogger Etkinleştirme:

******

→ Tuş vuruşları kaydedilmeye başlar.

✅ Dosya Yükleme:

# 

# 📎 Notlar

- QuasarRAT antivirüsler tarafından kötü amaçlı yazılım olarak algılanabilir.  
- Test ortamı dışında kullanılması yasal değildir.  
- Sunucu ve istemci şifreli iletişim kurabilir (TLS).  
- Ağ ortamında tespit edilmemesi için özel yapılandırmalar yapılabilir.