Crt.sh ve Httpx ile Gizli Alt Alan Adlarını Ortaya Çıkarma Rehberi

Dijital keşfin heyecan verici dünyasına hoş geldiniz! Bu yazıda, saldırganların ve güvenlik araştırmacılarının sıklıkla kullandığı iki güçlü aracın—crt.sh ve httpx'in—dinamik birlikteliğini keşfedeceğiz. Adeta bir siber hazine avı gibi, bu süreçte gizlenmiş alt alan adlarını bulacak, onları analiz edecek ve hedefin çevrimiçi varlıklarını daha net bir şekilde göreceğiz.

# Kullanacağımız Araçlar

Bu keşif operasyonu için iki açık kaynaklı araca ihtiyacımız var:  
1. crt.sh – Sertifika şeffaflık loglarını sorgulayarak alan adı ile ilişkili tüm alt alan adlarını listeler.  
2. httpx – Her bir alt alan adına istek göndererek, durum kodu, kullanılan teknolojiler ve sayfa başlığı gibi detayları gösterir.

# Kurulum Adımları

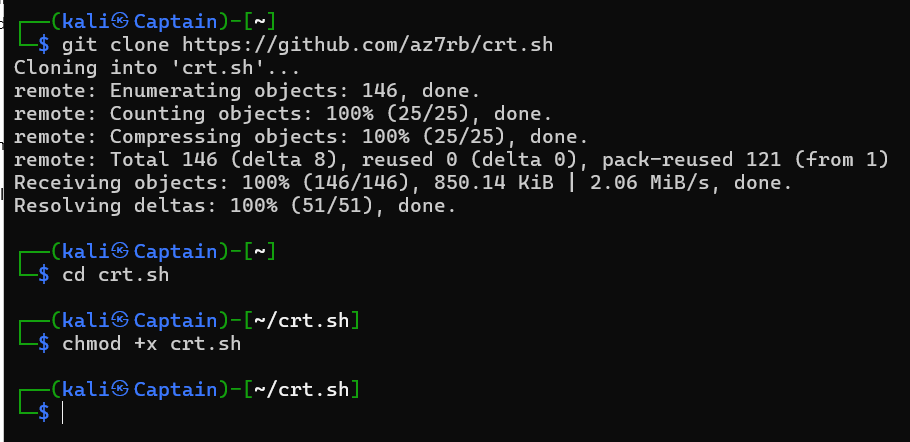
## 1. crt.sh Kurulumu

Aşağıdaki komutlarla crt.sh aracını kurabilirsiniz:

git clone https://github.com/az7rb/crt.sh

cd crt.sh

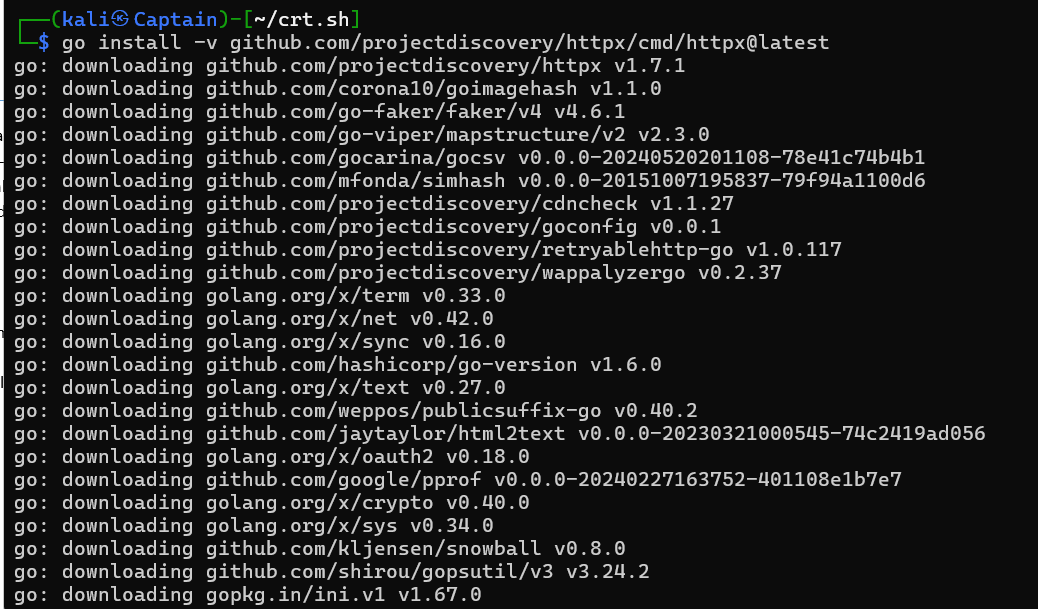
chmod +x crt.sh



## 2. httpx Kurulumu (Go ile)

Aşağıdaki komutla httpx'i yükleyebilirsiniz:

go install -v [github.com/projectdiscovery/httpx/cmd/httpx@latest](mailto:github.com/projectdiscovery/httpx/cmd/httpx@latest)



Go yüklü değilse, golang.org üzerinden kurulum yapabilirsiniz.

# Gerçek Dünya Örneği: Apple.com

Şimdi bu iki aracı birlikte kullanarak apple.com için canlı alt alan adlarını tespit edelim:

./crt.sh -d apple.com | httpx -title -tech-detect -status-code | grep 200



## Komut Açıklamaları:

- ./crt.sh -d apple.com: Sertifika loglarında apple.com’a ait alt alan adlarını çeker.

- httpx -title -tech-detect -status-code: Her alt alan adına istek gönderir, sayfa başlığını, kullanılan teknolojileri ve HTTP durum kodunu gösterir.

- grep 200: Sadece 200 OK durum koduna sahip, yani aktif ve erişilebilir alt alan adlarını filtreler.

# Neden Önemli?

Bu yöntem sayesinde:  
- Gizli veya unutulmuş alt alan adları keşfedilir.  
- Saldırı yüzeyi genişliği analiz edilir.  
- Güvenlik zafiyetleri için daha kapsamlı değerlendirme yapılır.  
  
Uyarı: Bu araçlar yalnızca yasal ve izinli ortamlarda kullanılmalıdır. İzinsiz tarama ve keşif işlemleri hukuki sonuçlar doğurabilir.

# Sonuç

Crt.sh ve Httpx, pasif bilgi toplamanın en etkili yollarından birini sunar. Doğru kullanıldığında, bir hedefin dijital varlıklarını görünür kılar ve siber güvenlik değerlendirmelerinde güçlü içgörüler sağlar. Siber keşif yolculuğunuzda başarılar!