**EvilURL Nedir?**

EvilURL, IDN (Internationalized Domain Name) homograf saldırılarını tespit ve analiz etmek amacıyla geliştirilmiş açık kaynaklı bir Python aracıdır. Homograf saldırıları, karakter benzerlikleri kullanılarak kullanıcıların kandırılması esasına dayanır. Örneğin:

* Gerçek: github.com
* Saldırı: ɡithub.com (Latin 'g' yerine benzer Unicode karakter)

EvilURL, böyle sahte URL’leri otomatik üretir, DNS çözümlemesi yapar ve tespit edilip edilmediğini kontrol eder.

**EvilURL ile Neler Yapabilirsiniz?**

* **Homograf domainler üretmek:** Orijinal domainle benzer karakterlerle mix edilmiş sahte URL’ler oluşturur.
* **DNS ve Punycode kontrolü:** Hangi URL’lerin aktif TLS kaydı olduğunu tespit eder.
* **JSON/tek tek raporlar:** Tekli domain veya toplu liste ile analiz yapılabilir
* **Topluluk destekli blok listesi:** Kullanıcılar tarafından paylaşılan zara7rlı domainler takip edilebilir.

**EvilURL Kurulum ve Kullanım Adımları**

**Kurulum:**

***git clone https://github.com/glaubermagal/evilurl.git***

***cd evilurl***

***python3 -m venv .venv***

***source .venv/bin/activate***

***pip install -r requirements.txt***

***pip install evilurl***

**Kullanım:**

**Tek tek domain kontrolü için: *evilurl github.com***

**Toplu liste kontrolü: *evilurl --file domains.txt***

***--domains-only:*** Sadece oluşturulan sahte domainleri gösterir.

***--log-full:*** Tüm varyasyonları ve DNS sonuçlarını listeler.

***--json:*** JSON formatında çıktı verir.

****

**homograph domain:** Görsel olarak benzer gözüken URL

**punycode:** Unicode karşılığının teknik gösterimi

**dns:** Bu domain aktif mi (IP'ye sahip mi)

**mixed:** Farklı karakter setlerinin karıştırılıp karıştırılmadığı

**Neden Bu Saldırıyı Öğrenmeliyiz?**

Kullanıcılar apple.com yerine аpple.com (Cyrillic 'а') gibi sahte adreslere yönlendirilebilir.

Homograf saldırıları hedefleme, kimlik avı (phishing) için yaygın kullanılır.

EvilURL, güvenlik açığı analizine erken adım olarak kullanılabilir.

**Korunmak İçin Yapılabilecekler:**

Tarayıcı güvenlik uyarılarını dikkatle değerlendir.

Organizasyonlarda sunucu taraflı bloklama uygulayın.

Güvenlik duvarlarına/IDS blok listeleri eklenebilir.

DNS loglarına homograf domainleri filtreleyecek kurallar ekleyin.

**Öğrenciler için Uygulama Alıştırması:**

Kendi seçtiğiniz popüler domainleri evilurl example.com ile analiz edin.

--domains-only parametresi ile sadece sahte URL’leri alın.

WHOIS veya DNS çözümleme ile aktif sahte domainler bulun.

Sınıfta bu domainleri tartışın; yapılabilecek güvenlik önlemlerini belirleyin.

EvilURL, IDN homograf saldırılarını keşfetmek ve analiz etmek için basit fakat güçlü bir araçtır. Özellikle siber güvenlik eğitimlerinde, **phishing farkındalığı** oluşturma ve **ilk adım saldırı testi** için idealdir. Elo başta not ettiğimiz IDN konseptini pekiştirmek için iyi bir pratiktir.