Her Gördüğüne İnanma

written by Mert SARICA | 1 November 2011

RTLO, namı diğer RIGHT-TO-LEFT OVERRIDE, Windows XP işletim sistemi kullanırken pek çoğumuzun dikkate almadığı ancak Windows Vista ve Windows 7 işletim sistemi kullanırken çok dikkatli olmamızı gerektiren bir Evrensel kod (unicode) karakteridir (\u202E). RTLO kısaca karakterlerin soldan sağa değil sağdan sola olarak işlem görmesini sağlar ve bu sayede sağdan sola yazılan diller (Arapça, İbranice, Süryanice vs.) desteklenebilmektedir.

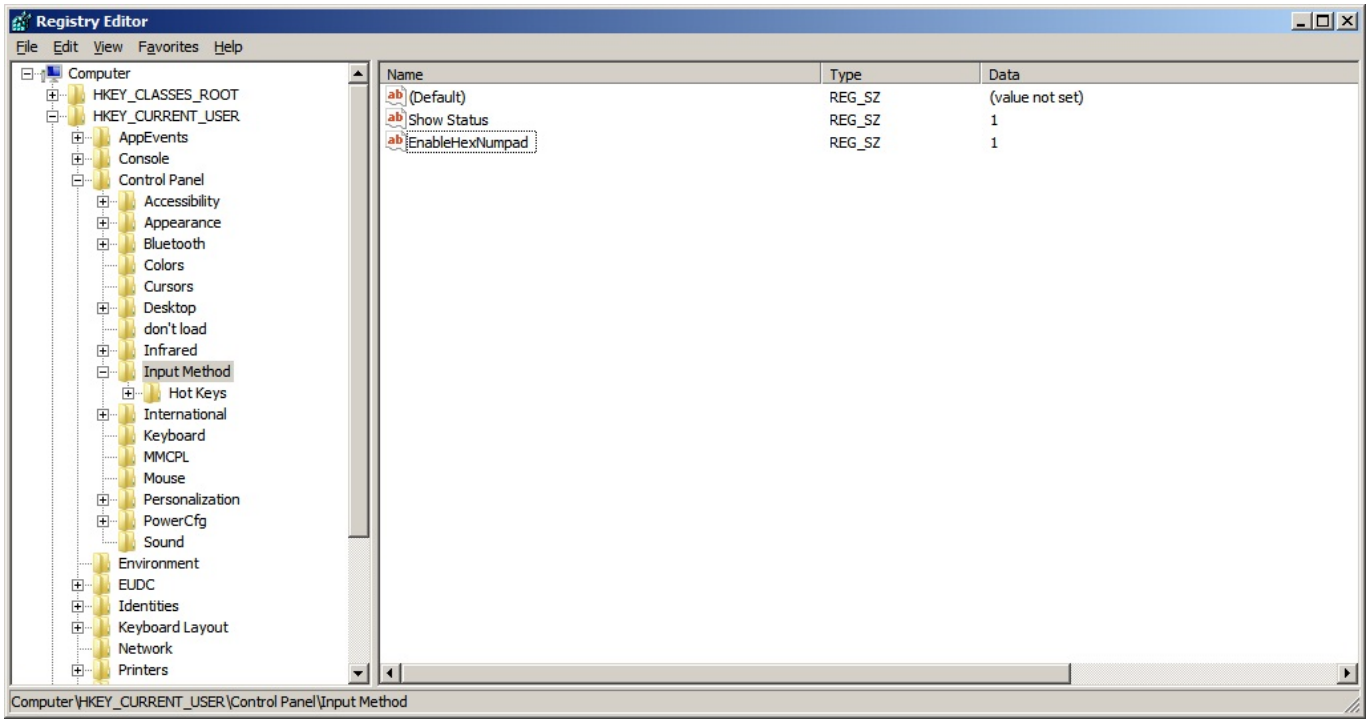
Windows XP işletim sistemi, varsayılan (default) olarak az önce bahsi geçen dilleri desteklememekte, ek bir paket yüklenerek (Install files for complex script and right-to-left languages) destekleyebilmekteydi. Ancak Windows Vista ve Windows 7 işletim sistemlerinin hayatımıza girmesi ile bu durum değişti ve varsayılan olarak bu diller desteklenir hale geldi. Peki bu desteğin bizimle ne ilgisi var ?

Yıllarca yakınımızdakiler tarafından yapılan şu şekilde uyarılara kulak kabarttık durduk, “Bir dosyayı çalıştırmadan önce uzantısına mutlaka dikkat et”, “Uzantısı exe ise sakın çalıştırma, virüs olabilir” ve bu sayede yıllar içinde hepimiz ister istemez bir dosyayı çalıştırmadan önce uzantısına dikkat eder olduk. Çoğu kimse farkında olmasa da bu kontrol sayesinde art niyetli kişiler zararlı yazılımları sistemlere bulaştırabilmek için daha farklı sosyal mühendislik yöntemlerine başvurmak zorunda kaldılar. Bu yöntemlerden biri de RTLO evrensel kod karakterli dosya adlarına sahip zararlı yazılımlar oluşturmak oldu. Peki bu dosya adlarını nasıl oluşturuyorlar da kullanıcıları kolaylıkla kandırabiliyorlar ?

Öncelikle RTLO evrensel kod karakteri içeren dosya adını Windows 7 işletim sistemi üzerinde oluşturabilmek için kayıt defterinde (registry) bir kaç değişiklik yapmak ve daha sonra sistemi yeniden başlatmak gerekiyor.

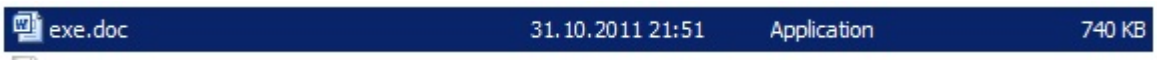
Bunun için izlenmesi gereken adımlar sırasıyla:

- Regedit komutu çalıştırılır. (Start -> Arama kutucuğu -> regedit)
- HKEY_CURRENT_USER\Control Panel\Input Method altında EnableHexNumpad anahtarı oluşturulur ve anahtara 1 değeri atanır.
- Sistem yeniden başlatılır.



Ardından .exe olan program uzantısının istenilen başka bir uzantıymış gibi görünmesi için RTLO evrensel kod karakterini dosya adında kullanıyorlar. Daha net olması adına ufak bir örnek üzerinden ilerleyelim.

- Windows/system32 klasörü altında yer alan calc.exe programını dilediğiniz bir klasöre kopyalayın.
- Programın uzantısının doc olarak görünmesini sağlayacağımız için programın simgesini (icon) Microsoft Word simgesi olarak değiştirin. (Resource Hacker programı işinizi görecektir.)
- Daha sonra programın adını (rename) cod.exe olarak değiştirin.
- Ardından programın adını tekrar değiştirmek için programın üzerine farenin sağ tuşu ile basıp menüden yeniden adlandır (rename) öğesini seçin.
- İmleci c harfinin başına (en sol) getirin ve ardından klavyeden NUMLOCK açık iken ALT ve FN tuşlarına basılı tutarak +202E tuşlarına basın.



Gördüğünüz üzere programın uzantısı artık doc olarak gözüküyor. Komut satırından programın bulunduğu klasörde DIR komutunu çalıştıracak olursanız bu yanılgının görüntüden ibaret olduğunu hemen anlayabilirsiniz.

```
20.11.2010  14:16           776.192 ?cod.exe
```

Python ile yukarıda bahsetmiş olduğum adımları (simge değiştirme hariç) otomatize eden RTLO.py isimli programa buradan ulaşabilirsiniz.

Programın kullanımı: python rtlo.py [extension] [source filename] [new filename]
Örnek kullanım: python rtlo.py .doc calc.exe Confidential_document_no_

Sonuç olarak Windows Vista veya Windows 7 kullanıcısıysanız ve eskiden kalma uzantı kontrolü yaparak programları gözü kapalı çalıştırma alışkanlığınız varsa yakın zamanda sıkıntı yaşama ihtimaline karşı programları çalıştırmadan önce içinde bulunduğu klasörde yer alan TYPE (Application ise dikkat!) kolonuna veya HEX Editör ile başlık bilgisine (ilk 2 bayt MZ ise dikkat!) dikkat etmeniz faydalı olacaktır.





Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim…