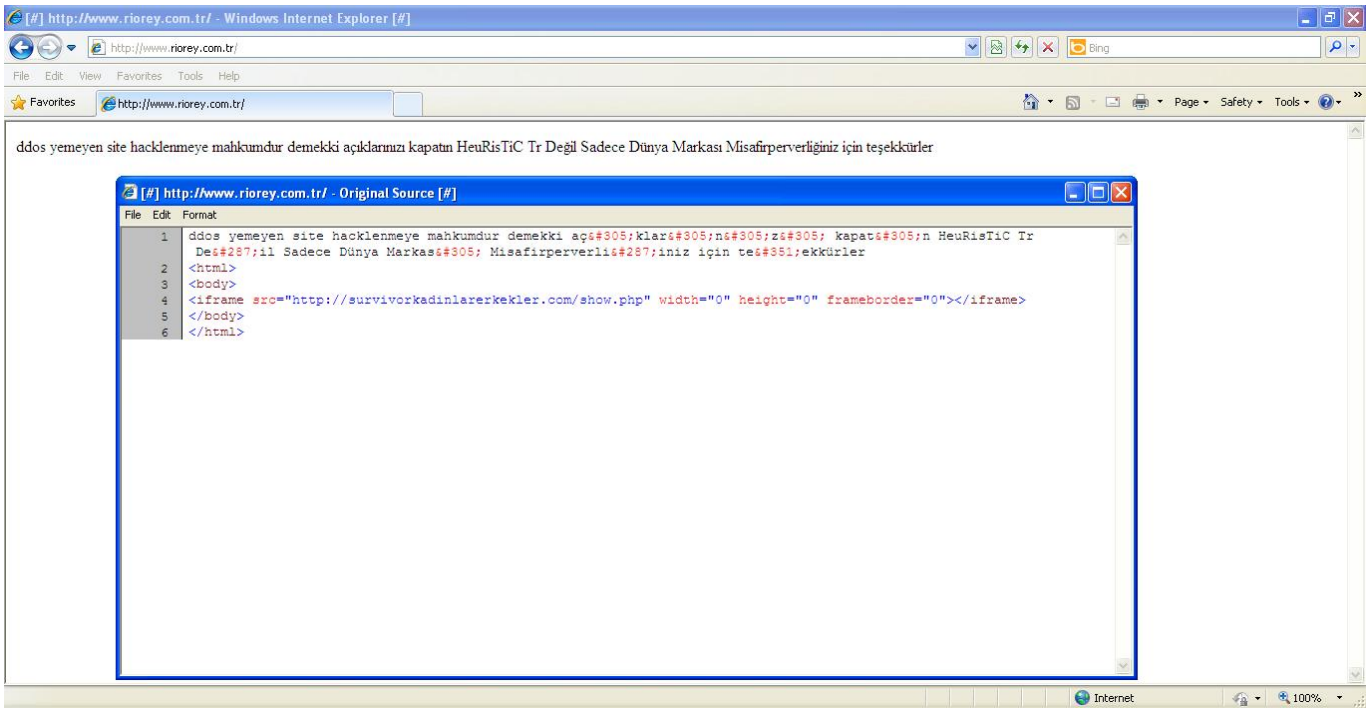
Riorey.com.tr Hacklendi

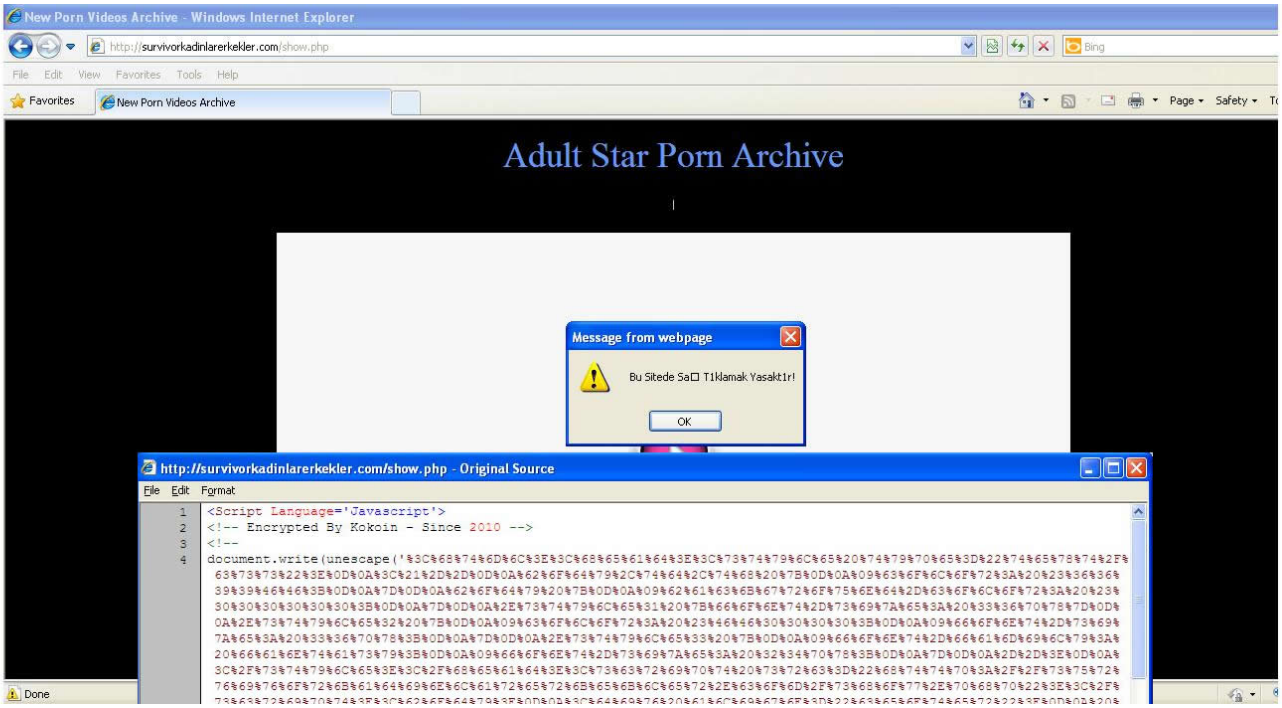
written by Mert SARICA | 29 June 2010

Huzeyfe bugün yayınladığı bir yazı ile Türkiye'de de ofis açmış olan DDoS ürün geliştiricisi Riorey firmasının TR uzantılı web sitesinin hack edildiğini duyurdu. Duyurmakla yetinmeyerek beni kaka yazılım inceleme uzmanı olarak lanse ederek benden bu siteye art niyetli kişiler tarafından yüklenmiş olan zararlı yazılımı incelememi talep etti ve bende alet çantamı kaptığım gibi olay yerinde incelememi gerçekleştirdim.

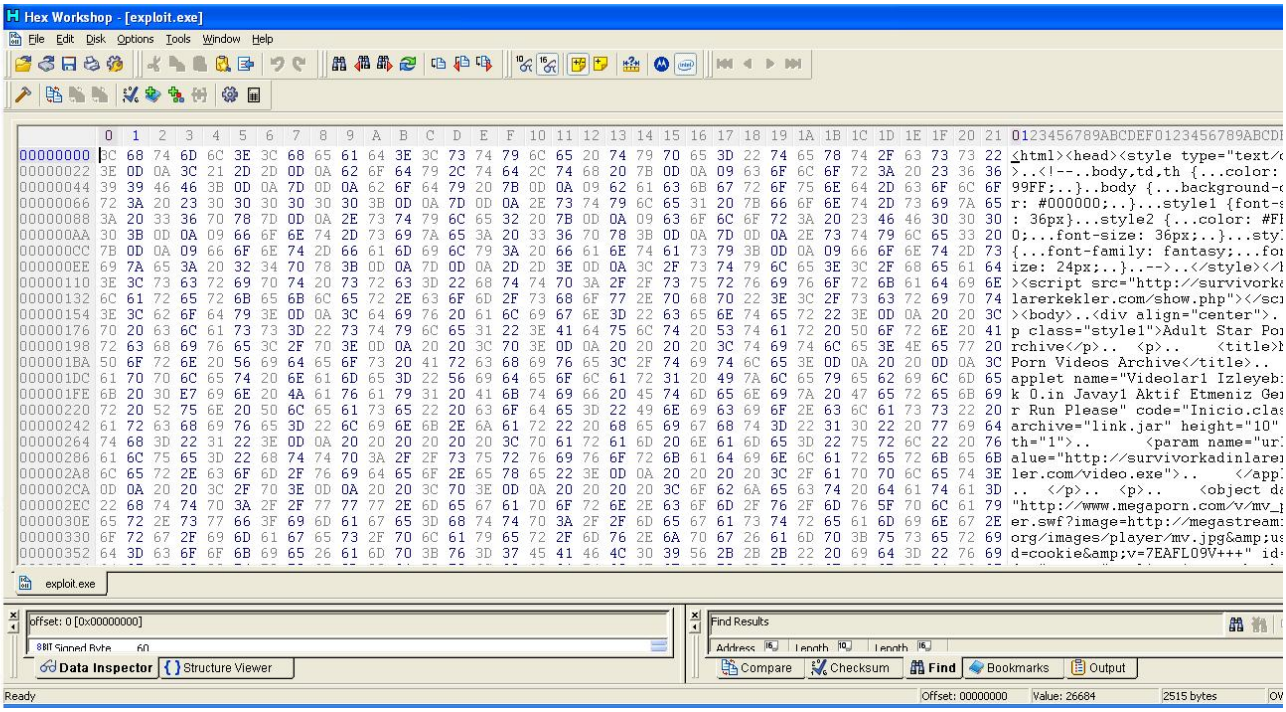
Aslında zararlı yazılım siteye direk olarak yüklenmemiş sadece zararlı yazılımı içeren başka bir siteye frame açılmıştı.



Frame açılan asıl siteyi ziyaret ettiğimde ise son zamanlarda oldukça sık rastladığım, daha önceki zararlı yazılım analizlerinde de bir çok defa yer verdiğim ve *Drive by download* yöntemiyle kullanıcıların işletim sistemine bulaşan bir trojan ile karşılaştım.



Her ne kadar sayfanın kaynak kodunda Encrypted yazıyor olsada Hex Editör ile değerleri incelediğimde öyle olmadığını gördüm. Daha önceki yazılarımı takip edenleriniz var ise *link.jar* ve *Inicio.class* JAVA dosyalarını anımsayacaklardır.

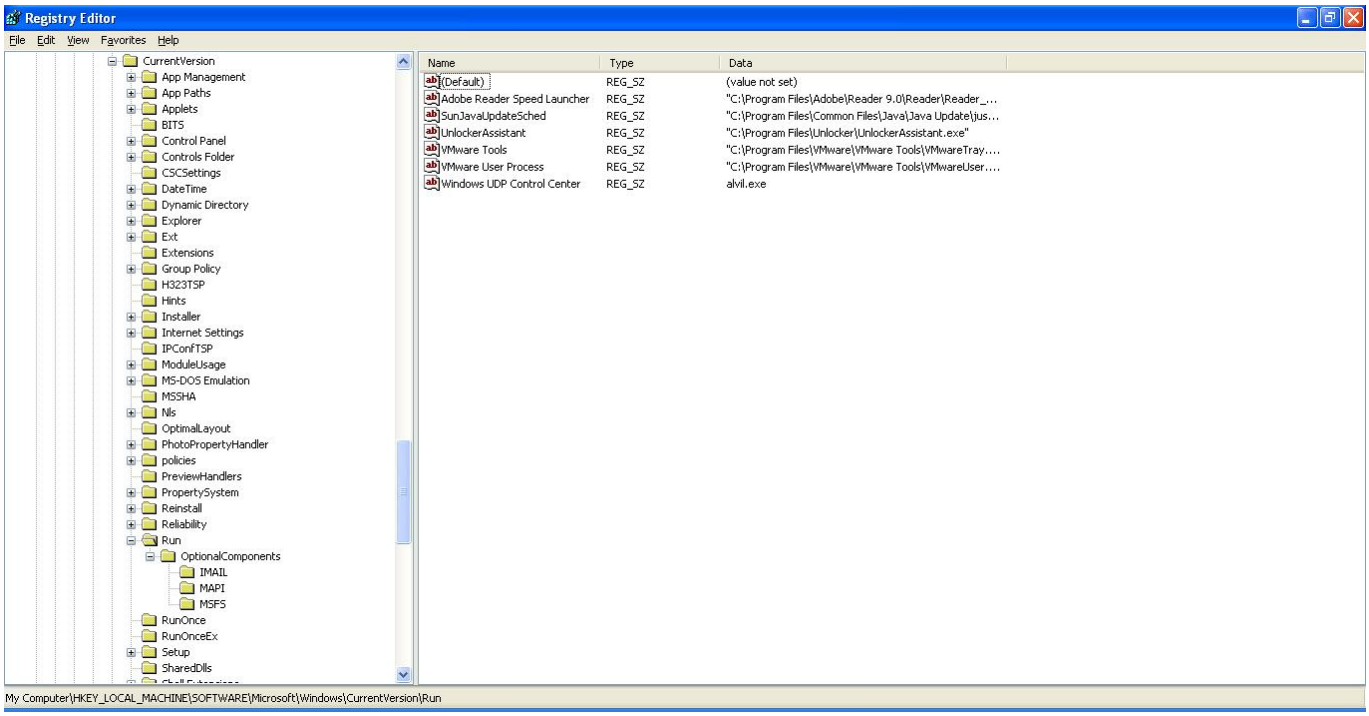


Yine daha öncekiler ile aynı yöntemi izleyen art niyetli kişiler, siteyi ziyaret eden kullanıcıların geçerli imzası olmayan link.jar JAVA uygulamasını çalıştırmaya zorlamakta ve uyarıyı görmezden gelerek kabul eden kullanıcıların işletim sistemine trojanı yüklemekteler.

Video.exe adındaki zararlı yazılımı çalıştırdığımda karşıma ilk olarak

ASProtect ile paketlenmiş olduğuna dair bir uyarı mesajı çıktı. ASProtect çoğunlukla art niyetli kişilerce zararlı yazılımlarının Antivirüs yazılımları tarafından yakalanmasını engellemek amacıyla kullanılmaktadır.

Bu mesajı geçtikten sonra bu defa hemen hemen çoğu zararlı yazılımda ayarlanan sahte hata mesajı (Picture can not be displayed.) ile karşılaştım. Bu mesajıda geçtikten sonra bu defa yazılımın kendisini *alvil.exe* adı altında Windows\system klasörü altına kopyaladığını ve ayrıca Windows yeniden başladığında her defasında tekrar çalışabilmek için kendisini kayıt defterinde (registry) *HKLM/Software/Microsoft/Windows/CurrentVersion/Run* altında Windows UDP Control Center anahtarı olarak kayıt etmektedir.



Wireshark yazılımı ile trafiği incelediğimde alvil.exe adındaki yazılımın *facebook-pic.co.cc* alan adını çözümlediğini ve daha sonra ilgili IP adresine 4455 numaralı bağlantı noktasından (port) bağlanmaya çalıştığını gördüm.

Bu zararlı yazılımı debugger ile incelediğimde ise “Lamer detected. coming back in 24hrs, download and update” metni ve IRC (Internet Relay Chat) komutları dikkatimi çekti. Bu metni arama motorunda arattığımda ise karşıma

çıkan ilk kayıt ise bunun SDBot adında bir arka kapı yazılımı olduğunu ortaya çıkarttı. Bu botun temel amacı art niyetli kişi tarafından belirtilen IRC sunucusuna bağlanmakta ve hedef sistemde çalıştırmak üzere art niyetli kişinin komut göndermesini beklemektedir. Verilen komut ile hedef sistem üzerine farklı zararlı kodlar yüklemek mümkündür. Ayrıca bu bot spam yapmak ve kendisini çoğaltmak amacıyla MSN üzerinden mesaj gönderebilmektedir.

Bu site üzerinde yer alan zararlı yazılım tarafından etkilendiğinizden şüphe ediyorsanız Windows\system klasörü altında yer alan alvil.exe adında dosyanın varlığını kontrol etmenizi öneririm. Kurumlar için ise *www.facebook-pic.co.cc* alan adı için geçmişte ve gelecekte yapılan DNS sorgularını kontrol etmelerini ve ayrıca *85.153.32.69* IP adresine doğru gerçekleşen tüm bağlantıları tespit etmelerini öneririm.

Bir sonraki yazıda görüşmek dileğiyle…